



El éxito o el fracaso de nuestras acciones forenses se debe en gran parte a las acciones mediante las cuales salvaguardamos los resultados y a las herramientas que usemos para su análisis, de poco sirve extraer numerosa información si desconocemos lo que estamos buscando. En este caso aunque existen numerosas herramientas de apoyo, solo la destreza del analista visualizará claramente las actividades delictivas frente a los usuarios inexpertos. Si bien cuanto mayor información sea extraída mayor será la información a analizar y mas herramientas podrán ser usadas para descubrir los elementos comprometidos pudiendo lanzar mas herramientas de contraste de los resultados, ya que algunas herramientas podrían mostrar resultados en forma de falsos positivos pero mostrar pistas que podriamos usar en otras.

Para el análisis del tráfico de red, la herramienta por excelencia a usar es Wireshark, que como destacamos en la unidad anterior, captura al configurar la tarjeta de red en modo promiscuo o sea que analiza todo el trafico sin discriminar la direccion MAC de origen o destino. Si el sistema está apagado es probable que no saquemos conclusiones de la maquina, dado que no existiría trafico de red activo.

Para el análisis de la máquina infectada existen numerosas herramientas, aunque sin duda la aplicación estrella es Nessus ya que tras el análisis realiza un resumen pormenorizado de los parches, plantillas de seguridad y emite un resumen en formato XML y HTML para ser exportado, el problema principal de Nessus es su precio ya que la versión Manager oscila entre los 2.920-4745 \$ en su tienda online a los 2.190 \$ de la versión Profesional que solo integra el análisis de vulnerabilidades. Por suerte al proceder dicha herramienta del mundo Open Source (código abierto) de Unix dispone también de una versión de evaluación que nos servirá para realizar nuestros analisis durante un tiempo limitado tras el registro. En la distribución de seguridad Kali Linux está disponible la versión gratuita para poder ser evaluada.

Como indicabamos Nessus no es la única herramienta de analisis de vulnerabilidades para sistemas Windows, Mac, Unix, Solaris , etc. la herramienta GFI LANGuard realiza las mismas funciones de análisis, aunque su precio de licencia es más moderado, no deja de ser un producto profesional que posee un alto coste habida cuenta de la especialización que requeriría su uso y análisis de los resultados obtenidos.

Pero dado que pretendemos que nuestro análisis sea accesible y gratuito; aunque mas complejo de interpretar; nos concentraremos en las herramientas disponibles, en este caso Autopsy que permite analizar los resultados y presentar un informe final de conclusiones, aunque como indicamos su aspecto y

ayudas es más espartano que las herramientas de pago dado que deberá conocer el último parche del sistema a analizar, la última vulnerabilidad declarada, etc. ya que la función de autopsy no es tan pormenorizada como las herramientas de pago. Aquí dispone de una guía para su uso.

Una de las herramientas más desconocidas y más implementadas en el seno de la AGE - Administración General de Estado es la herramienta CLARA que permite analizar pormenorizadamente el estado de las estaciones Windows de forma notoria y eficiente.

Aunque como es evidente al solo analizar los clientes bajo arquitecturas Windows perdemos la posibilidad de analizar máquinas con sistemas operativos UNIX, Mac, Solaris, etc. El licenciamiento de esta aplicación y su uso está regulado por la administración, particularmente por el CCN - Centro Criptológico Nacional.