Análisis de Malware en Entornos de Red Controlados

Introducción

En el presente caso práctico el estudiante tiene que usar un entorno virtual mediante el software de virtualización *VirtualBox* (https://www.virtualbox.org/), o bien puede utilizar *VMWare* (https://www.vmware.com/es.html) como alternativa en su versión libre. A la hora de realizar diversos análisis, puede ser esencial simular el comportamiento de los servicios existentes en una red para estudiar su funcionalidad su comportamiento en un entorno controlado y sin comprometer nuestra red física.

Pasos a seguir

1. Configura la máquina virtual de Ubuntu, de la Red Virtual Controlada creada en la actividad anterior, para que tenga de nuevo acceso a Internet, y así poder instalar software adicional.
2. Instala Wireshark y Tshark en dicha máquina virtual de Ubuntu:
   $ sudo apt-get install wireshark
   $ sudo apt-get install tshark
3. Descarga e instala, y describe brevemente, los siguientes programas en la máquina de Windows para inspeccionar malware. No es necesario que utilices todas, sólo las que creas que puedes necesitar para llevar a cabo los análisis oportunos.
   a. Process Hacker (http://processhacker.sourceforge.net/).
   b. Process Monitor (https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx).
   c. Noriben (https://github.com/Rurik/Noriben). Hace falta Python.
4. Reinicia los servicios de InetSim y Wireshark/Tshark, y comprueba que funcionan correctamente. Todo el software que se utilice debería tener privilegios de administrador.
5. Elige uno o varios ficheros de malware a nivel local y de red que consideres de entre la documentación del curso virtual, u otro que consideres de interés.
   a. *Muy importante:* no lo descargues desde la máquina virtual anfitriona y no lo ejecutes mientras sigas conectado a Internet (aunque sea dentro de la máquina virtual). Deberías hacerlo desde la máquina virtual de Ubuntu.
   b. Puedes utilizar ejemplos del libro "Practical Malware Analysis" (https://practicalmalwareanalysis.com/labs/), de los sitios web recomendados en el libro base, entre otros. Dicha documentación también está disponible en O'Really.
6. Vuelve a asilar la máquina virtual y la red del exterior, en modo *host-only*.
7. Deshabilita el Servicio de Windows Defender de la máquina Windows, ya que puede interferir cuando se ejecuta un malware. Se debe hacer en el editor de directivas de grupo local de Windows. Generalmente en *Configuración del equipo | Plantillas administrativas | Componentes de Windows | Windows Defender*. En el panel derecho, hacer doble click en *Desactivar la política de Windows Defender*.
8. Analiza dicho fichero de malware:
   a. Con Wireshark/Tshark.
   b. Con InetSim en ejecución.

9. Otra alternativa a InetSim es FakeNet-NG (https://github.com/fireeye/flare-fakenet-ng), que permite interceptar y redirigir todo o tráfico de red específico mediante la simulación de servicios de red. Si se considera oportuno, puede explorarse esta opción como alternativa, o complementario *(opcional)*.

Entrega

Sigue los pasos del caso práctico que haya desarrollado y realiza un informe sobre el mismo, problemas encontrados, y las conclusiones obtenidas. El informe debería ser no mayor de 10 páginas, y teniendo en cuenta que el destinatario es el jefe de un departamento técnico, que desea tomar decisiones técnicas.