Índice

Objetivo de la práctica

Durante el desarrollo de esta práctica, el alumno infectará una máquina virtual de Windows con un gusano. Los objetivos de la práctica son:

- Reconocer los gusanos como un proceso más del sistema operativo (si no se instala un *rootkit*)
- Localizar el gusano y eliminarlo del sistema de forma manual, sin utilizar un antivirus.

Preparación de una máquina virtual

Instalar un gusano es una operación *arriesgada*, por lo que no se recomienda utilizar la máquina real para esta práctica. Necesitaremos una máquina virtual con las siguientes características:

- Sistema operativo Windows 7,8 o 10
- No se necesitan más de 2G de memoria
- Conexión a Internet, para bajar el malware.
- Deberá tener *Windows Defender* y cualquier otro antivirus desactivado

Ejercicio 1 : Instalación del gusano (1 punto)

Descarga el gusano:

https://alvarogonzalezsotillo.github.io/apuntes-clase/seguridad-informatica-smr2dual/Worm.VBS.Dunihi.C/article_FB.vbs.zip

También se puede conseguir el gusano desde el fichero adjunto a este PDF.

El fichero está comprimido con la contraseña `virus`. Utiliza un programa como 7-Zip para descomprimirlo. Colócalo en el escritorio y ejecútalo.

Ejercicio 2 : Localización y eliminación del gusano (4 puntos)

Utiliza herramientas como procexp y autoruns para:

1. Localizar el programa del gusano
2. Localizar de qué forma se ejecuta cada vez que se inicia Windows
3. Detectar si el gusano se está comunicando con algún otro programa utilizando la red (*llamada a casa*)
4. Desactivar y eliminar el gusano

Ejercicio 3 : Eliminación del gusano por un antivirus (2 puntos)

Vuelve a instalar el gusano. Después, instala un antivirus y observa cómo detecta y elimina el gusano. Es posible que necesites ejecutar una búsqueda manual de todo el disco.

Ejercicio 4 : Contagia un *pen drive* (3 puntos)

Precaución

Utiliza una memoria USB que no contenga datos importantes, porque por seguridad deberá formatearse al finalizar la práctica.

Conecta la unidad USB a la máquina virtual y:

- Desactiva o desinstala el antivirus.
- Crea dos archivos de texto en el directorio raiz del USB, y dos directorios. Cada uno de los dos directorios tendrá a su vez otros dos ficheros.
- Vuelve a instalar el gusano con la unidad USB aún conectada.
- Observa los cambios que se han producido en la unidad USB. Descríbelos en el trabajo.
- Desinstala de nuevo el gusado del disco duro.
- Desinstala el gusano de la unidad USB.

Precaución

Aunque creas que has desinstalado el gusano del la unidad USB, formatéala para mayor seguridad

Qué se valorará

El trabajo debe ser un ***tutorial*** de cómo localizar manualmente un *malware*. Por tanto, no es correcto:

- Incluir los enunciados en el trabajo
- Simplemente, poner pantallazos

Se valorará:

- Que cada paso quede bien documentado.
- La corrección técnica (que funcione)
- Que esté correctamente redactado, de forma que nuestro lector lo entienda
- La apariencia profesional:
  - Estética
  - Organización
  - Homogeneidad de formatos y estilos

Instrucciones de entrega

- El ejercicio se realizará y entregará de manera individual.
  - Solo se admiten trabajos en pareja, si en clase es necesario compartir ordenador.
  - En este caso, todos los integrantes del grupo deben subir el trabajo al aula virtual.
- Los trabajos pueden entregarse:
  - Como una entrada en un blog (preferido)
  - En formato **DOC** o **DOCX**.
  - En formato **ODT**.
  - En formato **PDF**.
- La entrega se realizará en la tarea correspondiente del aula virtual. Si se entrega un fichero, este se subirá directamente. Si es una entrada de blog, se subirá un fichero de texto con la URL de dicha entrada.