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 virus
- Deberá tener *Windows Defender* y cualquier otro antivirus desactivado

Instalación del gusano (1 punto)

Descarga el gusano de cualquiera de las siguientes direcciones:

- `https://alvarogonzalezsotillo.github.io/seguridad-informatica-smr2dual/Worm.VBS.Dunihi.C/article_FB.vbs.zip`: Fichero comprimido con la contraseña `virus`, para evitar problemas con los antivirus
- `https://alvarogonzalezsotillo.github.io/seguridad-informatica-smr2dual/Worm.VBS.Dunihi.C/article_FB.vbs`: El gusano sin comprimir

Colócalo en el escritorio y ejecútalo.

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
4. Desactivar y eliminar el gusano

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.

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 como para que nuestro lector lo entienda
- La apariencia profesional del análisis:
  - 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.
  - Los trabajos pueden entregarse:
    - En formato **DOC** o **DOCX**.
    - En formato **ODT**.
    - En formato **PDF**.
    - Como una entrada en un blog (*novedad*)

  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.