**¡Virus!**

**La OMSI (Organización Mundial de la Salud Informática) acaba de establecer una nueva pandemia, no de Covid ni ninguno de esos diminutos entes biológicos sino de… ¡virus informáticos!**

En realidad, se habla genéricamente de "virus", pero hay un amplio abanico de programas maliciosos que contagian las computadoras. La OMSI nos encarga modelizar y simular ciertas situaciones de ataques informáticos, el impacto que provocan y cómo se responde.

**Programación**

En las computadoras hay programas que en principio están sanos y que se pueden ejecutar sin problemas. No nos interesa representar a utilidad práctica en sí de cada programa o cómo es su interacción con el usuario, sino ciertas características vinculadas al uso de los recursos internos del equipo.

**Arquitectura**

Todo programa ocupa siempre una parte del disco de la computadora. Cuando está en ejecución utiliza una cierta cantidad de memoria. Por otra parte, se conoce el tamaño total del disco y de la memoria de la computadora.

**Se pide hacer:**

* Instalar un programa. Se debe registrar lo que sea necesario para que luego el programa pueda ejecutarse. En caso de no haber lugar suficiente en el disco, se debe advertir adecuadamente y no completar la instalación.
* Ejecutar un programa. Hace que un programa funcione, haciendo uso de la memoria requerida. Además, debe estar instalado y no estar ya en ejecución. En caso de no contar con la memoria necesaria, no se ejecuta el programa. Además, se lleva el registro de cuantas veces fue ejecutado un programa en la máquina.
* Detener un programa. Hace que un programa en ejecución se detenga, liberando los recursos que utilizaba.
* Estadísticas de uso:
  + El programa en ejecución que más memoria consume
  + Si hay algún programa instalado que ocupe más de la mitad del disco
  + Considerando un conjunto de computadoras, encontrar las que en ellas se puede instalar un programa dado.

**Sistemas operativos**

Existen también sistemas operativos, que son programas que tienen una utilidad especial.

Hay inicialmente uno instalado en la computadora, pero se lo puede desinstalar e instalar otro sistema operativo en su lugar. Si no está en ejecución, no se puede ejecutar ningún otro programa. Y cuando se detiene su ejecución, todos los demás programas en ejecución también se detienen.

Reformular lo que sea necesario para contemplar la presencia de los sistemas operativos

**Programas maliciosos**

Hay algunos que son maliciosos y que pueden infectar a cualquier otro programa. Los programas maliciosos no se instalan, pero pueden "hospedarse" en otros programas instalados. Cada programa puede hacer de programa hospedador para otros programas, por lo que el espacio de disco que ocupa debe contemplar también lo que ocupan los programas maliciosos que hospede.

Al ejecutarse el programa original se ejecutan de forma automática todos los programas maliciosos hospedados en él por lo que se pasa a consumir también sus correspondientes recursos.

Al detenerse el programa hospedador, los programas hospedados no se detienen sino que continúan en ejecución.

Nos vamos a concentrar en los siguientes programas maliciosos:

* Troyano: al ejecutarse, abre el puerto 80 en el sistema de forma irrestricta, lo cual hace que la máquina quede vulnerable a ataques.
* Virus: al ejecutarse, infecta a otros programas instalados en la máquina, hospedándose en ellos. Para ello, selecciona a los programas que se hayan ejecutado más cantidad de veces que la propia potencia del virus. Si el programa a infectar ya estuviera infectado por el mismo virus, no lo infecta nuevamente.
* Destructor: al ejecutarse desinstala el primer programa que está actualmente corriendo en el sistema. Sin embargo, al ejecutarse una determinada cantidad de veces, que puede ser diferente entre un destructor y otro, no vuelve a desinstalar más nada, sólo queda hospedado en el programa que infectó, consumiendo recursos.
* Inventar un nuevo tipo de programa malicioso que sea muy similar a uno anterior pero con una diferencia no trivial en la lógica
* Worm: es un programa que además tiene un payload (en castellano, “cacho de código”) que ejecuta cada vez que el programa hospedador se ejecuta y que puede hacer un efecto arbitrario sobre la máquina. Cada worm se programa de forma distinta y puede tener efectos distintos (Item bonus)

**Se solicita:**

* Saber si un programa es sano, lo que se da cuando no está infectado por nadie
* Hacer las adaptaciones necesarias para que los programas maliciosos puedan infectar otros programas, escribiendo al menos un test que muestre el funcionamiento de cada tipo una vez infectado. Todos los puntos de la primera parte deben seguir funcionando correctamente.
* Saber cuáles son los 3 virus de mayor impacto entre un conjunto de virus, donde el impacto según la OMSI es la cantidad de programas infectados en la computadora.

**¡Antivirus!**

También existen ciertos programas que al ejecutarse nos permiten limpiar un programa de infecciones. Cada uno conoce qué programas maliciosos sabe eliminar. Por ejemplo, el UTNAV sabe eliminar tanto el W32.antipdepv como el OSX.paraosc. Eliminar un programa malicioso implica detener su ejecución y "deshospedarlo" del programa infectado. Además, todo antivirus cierra los puertos abiertos (igual, ojo! ejecutar nuevamente un virus podría volverlo a abrir)

**Se solicita:**

Instalar y ejecutar un antivirus y que hagan lo esperado

**Para pensar**

Sin escribir todo el código nuevo, explicar y definir al menos 2 conceptos de la materia nos podrían servir para que se pueda

* soportar un nuevo tipo de destructor que sobrevive hasta N corridas de antivirus
* soportar un nuevo tipo de troyano que sólo puede ser eliminado si ya corrió y explicar brevemente cómo se implementaría considerando ambos conceptos

¿Qué pasaría si los programas maliciosos o los mismos antivirus pudieran infectarse por otros programas maliciosos, que también se ejecuten automáticamente y consuman recursos? ¿Qué cambios habría que hacer para que esto funcione?