Universidad de Costa Rica
Sede del Atlántico
Bachillerato en Informática Empresarial
IF-6000 Redes en los negocios
II Semestre, 2020
Profesor: Dr. Antonio González Torres

Proyecto de investigación y desarrollo

Valor: 12.5%
Fechas de entrega: 11 de noviembre
Criterios de evaluación: La investigación se debe realizar grupos de cuatro personas

Descripción

Los virus pueden infectar a las computadoras de diversas formas, pero la más común es mediante archivos que descargamos de Internet o que llegan a través de nuestros correos electrónicos. Un virus, que también es un programa, puede modificar o eliminar archivos, así como afectar el rendimiento de nuestra computadora. Estos programas también pueden enviar nuestros datos y archivos confidenciales a otra persona o permitir que alguien tome el control de nuestra computadora de forma remota y la use para sus propios fines. Por lo que el uso de un software antivirus es imprescindible para mantener protegidos nuestros activos digitales y equipos.

Funcionamiento básico de los antivirus

El software antivirus cuenta con una base de datos con las firmas de archivos (hash) que han sido detectados como peligrosos. Además, revisan los patrones de archivos y páginas web para verificar si se encuentran registrados como potencialmente peligrosos. Cuando un archivo es recibido se le calcula el hash y se compara con los que están registrados en la base de datos, si coincide con alguno de ellos se mueve a la zona de cuarentena para que no se infecten otros archivos en el sistema.

El escaneo de archivos se puede realizar de forma automática y en tiempo real, cuando la computadora recibe un archivo. Sin embargo, también se pueden realizar revisiones por demanda y de forma programada. El primer tipo de revisiones la activa el usuario haciendo clic sobre un botón con la etiqueta Escanear Ahora, mientras que el segundo tipo de revisiones se pueden programar para un día y hora especifica.

Requerimientos

El sistema antivirus se debe desarrollar usando Python y debe contar con los siguientes elementos:

Servidor: El servidor cuenta con la base de datos con las firmas de archivos registrados como peligrosos, y se mantiene esperando por peticiones. Se utilizará MD5 para calcular la firma de los archivos. Además, mantiene una base de datos con el registro de los clientes activos y los archivos que ha detectado cada uno de los clientes como peligrosos. El servidor funciona de forma centralizada.

Cliente: El cliente se conecta al servidor al iniciar y registra su dirección IP, y el servidor le envía la base de datos de firmas. Asimismo, el cliente envía la información de los virus detectados al servidor. El cliente funciona de forma residente en cada computadora cliente y es un proceso que se ejecuta de forma indefinida.

La comunicación entre el cliente y el servidor se debe realizar usando sockets.

Consideraciones

1. El cliente y el servidor se deben integrar para que el proyecto sea sujeto de revisión.
2. Si el código no se ejecuta sin errores, no se evaluará el resto de entregables.
3. La documentación del proyecto debe estar completa para que este sea sujeto de revisión.

Documentación

1. Para administrar cada entregable se usará un repositorio GitHub separado.
2. El Readme de cada repositorio tendrá una descripción del software que se debe instalar para ejecutar el proyecto y los pasos detallados para que un programador pueda hacer cambios. Esta información servirá como documentación técnica.
3. La Wiki de cada proyecto debe contener la descripción del trabajo y las historias de usuario que fueron elaboradas.
4. En el repositorio de Github se indicarán las tareas que se están realizando, el estado de estas, y el responsable de ejecutarlas. Para asignar el responsable, las tareas se deben convertir a un issue.
5. La Wiki debe incluir un manual de usuario detallado que explique los pasos necesarios para utilizar el programa.

Calificación

1. La entrega del código fuente ejecutable (sin errores) tiene un valor de 70 puntos.
2. La documentación tiene un valor de 30 puntos: 9 puntos para el manual técnico (Readme), 12 puntos para la descripción, historias de usuario, tareas y asignación de tareas (Wiki) y 9 puntos para el manual de usuario (Wiki).

Política de ética y transparencia

Los trabajos presentados por cada grupo son originales. Si han recibido ayuda de algún compañero de clase o de alguien externo a la clase debe indicarlo en la documentación del trabajo. Asimismo, debe indicar los sitios web de donde tomaron ejemplos o código fuente. No informar sobre lo anterior podría ser una falta al reglamento de la universidad y su trabajo podría ser penalizado como una copia.