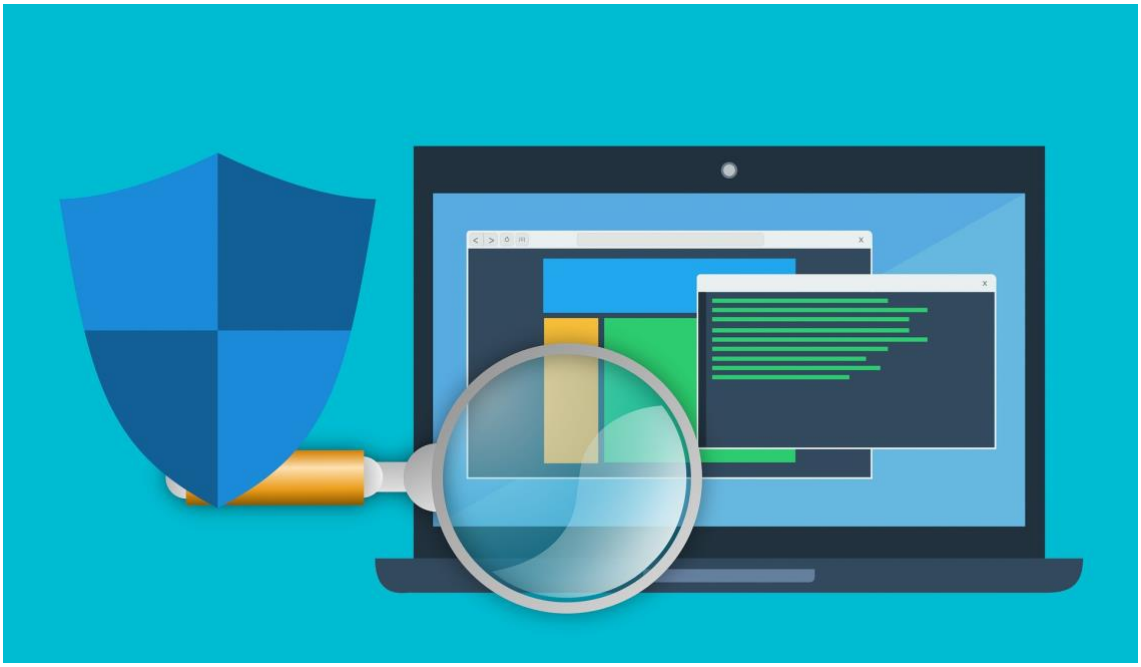

TRABAJO 7 ACTUALIZACIONES, APLICACIONES MALICIOSAS Y ANTIVIRUS

Seguridad Informática

Criterios de evaluación trabajados

3.3 Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.
3.4 Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.
3.5 Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.

David Romero Santos

Tabla de contenido

Descripción de la tarea

La seguridad informática referente al software es un dolor de cabeza continuo para usuarios y administradores prácticamente desde que se democratizó el uso de Internet. Probablemente este aspecto de la seguridad es el primero en el que piensa la mayor parte de la ciudadanía cuando hablamos de seguridad informática.

La historia del malware (programa maligno) se remonta a principios de los años 70, con la programación del primer virus:
https://www.xataka.com/historia-tecnologica/la-historia-de-creeper-el-primer-virus-informatico-jamas-programado

Desde entonces ha ido evolucionando y adquiriendo nuevas formas. Puedes consultar una infografía en la siguiente web referente a los principales hitos de malware en la historia:
https://www.welivesecurity.com/la-es/2016/10/24/historia-del-malware-actualizada/

Es necesario asumir que nunca podremos estar seguros del todo, y para evitar estar infectados, las principales acciones que podemos realizar son:

- Mantener nuestro sistemas y aplicaciones actualizados.
- Controlar la instalación de software, confiando solamente en aplicaciones originales y verificadas.
- Usar alguna aplicación antimalware fiable.
- Sobre todo, usar el sentido común cuando naveguemos por la red.

En este trabajo aprenderemos a asesorar a nuestros clientes sobre las actualizaciones del sistema y la verificación de aplicaciones. También veremos cómo actuar con archivos sospechosos y qué opciones tenemos para proteger activamente distintos sistemas operativos.

Actualiza el sistema

Realiza tutorial para un cliente sobre cómo actualizar los siguientes sistemas operativos: Windows, Linux, macOS, Android e iOS. Utiliza capturas propias en al menos dos de ellos.

Verifica el origen de las aplicaciones

Conocer el origen y la autenticidad de una aplicación a través de un ejecutable es muy complicado. Por eso, los sistemas operativos modernos confían o no en una aplicación si ha sido incluido previamente en una lista verificada por ellos. Es lo que conocemos como tienda de aplicaciones. Supuestamente, si instalamos una aplicación a través de una tienda de aplicaciones oficial (“Microsoft Store” en el caso de Windows, “Centro de software de Ubuntu” en el caso de Linux Ubuntu, “App Store” en el caso de macOS e iOS y “Play Store” en el caso de Android) será una aplicación verificada. Sabemos que esto no es así siempre, ya que se han dado caso de aplicaciones infectadas con malware en la Play Store por ejemplo, pero si se acotan muchísimo las probabilidades de vernos afectados si solamente instalamos aplicaciones de las tiendas oficiales.

Muchas veces queremos utilizar una aplicación que no está registrada en ninguna tienda, por lo que nos descargamos el ejecutable de algún lugar. Podemos identificar los ejecutables por su extensión:

.exe en sistemas Windows
.bin .rpm .deb .sh (y muchos más) en sistemas Linux
.dmg y .app en sistemas macOS
.apk en sistemas Android
.ipa en sistemas iOS

iOS es el único sistema operativo de los listados que no permite instalar aplicaciones fuera de su tienda oficial, a menos que tengas una cuenta de desarrollador (En Android y macOS solamente debes cambiar la configuración de seguridad para que te lo permita). En el resto de casos, la forma más efectiva de saber si una aplicación es confiable, es aplicar el sentido común a la hora de navegar y descargarla, haciéndolo siempre desde su sitio web oficial.

Como reconocer el sitio web oficial requiere cierta experiencia, una buena práctica es analizar el archivo ejecutable antes de instalarlo. La plataforma VirusTotal fue adquiridad por Google y permite analizar cualquier tipo de archivo o URL con múltiples motores, obteniendo detalles y advertencias sobre su uso. Puede obtener falsos positivos y negativos, pero es un buen punto de partida para comenzar a confiar en una aplicación.

Busca en Internet al menos dos archivos .exe y dos archivos .apk. Analízalos con: https://www.virustotal.com/es/

Elabora un informe sobre los detalles importantes que has podido obtener sobre esos ejecutables en la plataforma, indicando si confiarías o no en su origen.

Mantén tu sistema protegido con un antivirus

Tener instalado un antivirus es casi la principal preocupación de un usuario cuando adquiere un nuevo equipo. ¿Cuántas veces te han preguntado qué antivirus instalar solo por el hecho de saber algo de informática?

También escuchamos continuamente mitos urbanos como que macOS y Linux están libres de virus mientras Windows está lleno de ellos. Sí es verdad que a lo largo de muchos años se han escuchado muchas noticias sobre virus en Windows pero… ¿Cuánta gente utilizaba otro sistema? Si fueses un hacker dispuesto a programar un virus, probablemente querrías hacerlo para el sistema operativo que utilice más gente y así poder infectar más equipos.

La realidad es que los sistemas basados en Linux (como Android y macOS) si tienen una importante ventaja frente a los clásicos sistemas basados en Windows, y es que las aplicaciones están aisladas entre sí. Esto provoca que sea difícil acceder a otra aplicación desde una de ellas y hace más complicado que funcione un virus. Esto no quiere decir que sean sistemas inmunes.

Si entramos en la Play Store de un móvil Android y buscamos un antivirus, vamos a tener disponibles muchos. Pero claro, si una aplicación no puede entrar en otra… ¿Cómo puede un antivirus analizar otras aplicaciones? Es por eso que la mayoría de antivirus que encontramos en Android no hace nada más aparte de mostrarnos publicidad y una bonita animación de búsqueda de virus (que realmente no actúa como tal).

A continuación, os daré unas recomendaciones totalmente subjetivas a la hora de elegir el antivirus de un sistema operativo:

- Windows. Es el que más opciones tiene. Sin embargo, si no se va a optar por un antivirus de pago, es conveniente utilizar el que viene instalado por defecto en Windows 10, Windows Defender. Este antivirus ha mejorado mucho en las últimas versiones y es más que suficiente para una protección básica. Instalarle a un cliente un antivirus de pago en su versión gratuita solamente le traerá, en el mejor de los casos, publicidad intrusiva. Y en el peor de ellos, sobrecarga de los recursos del ordenador.
- Android. No te dejes engañar por los falsos antivirus. Lo importante en este caso es instalar solamente aplicaciones de la tienda usando el sentido común y, eso sí, revisar los permisos concedidos a las aplicaciones. Si tenemos una aplicación para hacer fotos… ¿Por qué necesita permiso del micrófono? Para revisar la configuración, confiabilidad y actualización de aplicaciones, la OSI creó una aplicación bastante buena que puedes probar: Conan Mobile (https://www.osi.es/es/conan-mobile). Es la único que recomiendo para este sistema.
- macOS e iOS. Por la idiosincrasia de estos sistemas operativos, lo único que aconsejo es aplicar el sentido común, no instalar aplicaciones desconocidas y, sobre todo, mantenerlos actualizados.
- Linux y servidores. Es bueno cuando administramos sistemas tener algún tipo de motor antivirus, por lo que pueda ocurrir, ya que no somos los únicos usuarios del mismo. En este trabajo vamos a probar clamAV.

clamAV es un antivirus totalmente gratuito y open source, esto nos garantiza una comunidad de desarrolladores que lo mantiene actualizado y atentos a cualquier nueva amenaza que pueda surgir.

Elabora un tutorial de instalación, uso y actualización del antivirus clamAV en Ubuntu Server.

Formato de entrega

Deberás entregar el documento con todo lo pedido en PDF, dentro de la tarea correspondiente.

La fecha de entrega es el **XX de XXXX**. Se utilizarán cinco sesiones completas en clase para realizarlo.

Evaluación

La calificación de cada criterio se calculará a partir de las siguientes rúbricas.

CE 3.3

Criterio	Puntuación
El alumno realiza un tutorial sobre como actualizar cinco sistemas operativos, utilizando capturas propias en al menos dos de ellos	5 puntos
El tutorial sobre cómo actualizar Windows es correcto y está bien explicado	1 punto
El tutorial sobre cómo actualizar Linux es correcto y está bien explicado	1 punto
El tutorial sobre cómo actualizar macos es correcto y está bien explicado	1 punto
El tutorial sobre cómo actualizar Android es correcto y está bien explicado	1 punto
El tutorial sobre cómo actualizar iOS es correcto y está bien explicado	1 punto

CE 3.4

Criterio	Puntuación
El alumno demuestra haber analizado el origen de al menos cuatro archivos	5 puntos
El alumno argumenta la confianza de los archivos con datos objetivos y subjetivos basados en el sentido común	5 puntos

CE 3.5

Criterio	Puntuación
El alumno realiza un tutorial bien explicado	5 puntos
El alumno se apoya en capturas de pantallas propias con marca de agua	5 puntos