VULNERABILIDADES EN LOS PRINCIPALES SS.OO.

Daniel Camba Lamas

Diego Casanova José

Román Puga Quintairos

ÍNDICE

INTRODUCCIÓN

Tal y como podemos ver en la NVD hay más de 70000 vulnerabilidades identificadas entre todos los sistemas operativos, de esas 70000 hemos escogido las más relevantes y algunas anecdóticas para entender con ellas que ningún sistema es impenetrable.

Así podremos analizar cómo ha evolucionado la seguridad de las tres plataformas y, en consecuencia, extraer conclusiones sobre las precauciones y buenas prácticas a tener en cuenta para evitar vulnerabilidades en la medida de lo posible.

MAC

Introducción.

El crecimiento de apple en la última década y pasar a convertirse en el punto de mira de casi todos, ha generado interés en los maleantes cibernéticos, por lo que hace poco vimos el primer *ataque de Ransomware*, pero aún siendo uno de los fallos más sonados del sistema de la manzana, no ha sido el único. A continuación exponemos los 5 más destacados, a partir de OSX 10.0.

Vulnerabilidades.

RENEPO

Cuyo nombre viene por ser el inverso de "Opener", se creó en 2004 y era el primer código malicioso desarrollado especificamente para OSX. Consistía en un gusano de secuencia de comandos *Shell* especializado en permitir a los intrusos robar información de los equipos donde este se asentaba, además de, desactivar actualizaciones, desactivar el firewall y descifrar contraseñas.

Actualmente todas las versiones activas del sistema tienen parcheado el método de ejecución de este tipo de virus.

KERANGER

A través del popular software de torrents Transmission ha sido difundido el primer caso de ransomware en Mac OS X. KeRanger se encarga de secuestrar los datos alojados en tu disco y luego te redirige a una página para obligarte a pagar si deseas que te sea desbloqueado. De alguna forma, se consiguió acceso a los servidores oficiales de Transmission, donde se sustituyó el software original por el software modificado que incluía el programa encargado de secuestrar los datos.

Actualizar la aplicación de "transmission" donde se ha aplicado el parche para esta seria vulnerabilidad.

DROPBOX

Cuando acudimos a "preferencias del sistema" en "seguridad y privacidad", donde dentro de la pestaña "privacidad". Aquí, las apps con acceso a "Accesibilidad", tienen acceso total al sistema, pues

Dropbox, se aprovechaba de una vulnerabilidad en la bd de usuarios de local de OSX.

Este fallo de seguridad sólo se dio en OSX anteriores a Sierra, antes de renombrarse como MacOS, por lo que con actualizar el sistema desde la AppStore, sería suficiente, aún así, Dropbox ya ha reculado y hace las cosas solicitando permisos.

GATEKEEPER

Gatekeeper, introducido en Mountain Lion (OS X 10.8), restringe la instalación y apertura de programas, si es que estos no fueron debidamente verificadas por los desarrolladores. El problema está en que este sistema sólo verifica el paquete una vez y "por fuera". El investigador Patrick Wardle utilizando un archivo confiable provisto por la propia Kaspersky Lab, Cuando la imagen de disco logra pasar la revisión, el archivo confiable comienza a hacer su trabajo ejecutando los archivos maliciosos del paquete. Éstos a su vez se encargarán de instalar malware con la capacidad para robar contraseñas, tomar el control del micrófono y la cámara web e incluso darle acceso remoto al atacante.

El problema fue solucionado en OSX 10.11 "El Capitán", como parche de seguridad general del sistema.

FLASHBACK

El mismo se hacía pasar por el programa de instalación de Adobe Flash, lo que, aprovechando una vulnerabilidad de Java, acabaría robando datos personales a los atacados, entre los que se encuentran su información bancaria y la redirección del motor de búsqueda hacia contenido malicioso.

Evolución y conclusiones sobre el sistema.

Los sistemas OSX siempre han podido presumir de una mayor seguridad, frente a equipos windows, pero la realidad era que esa seguridad derivaba de falta de interés por parte de atacantes hacia la plataforma, con el crecimiento de la última década apple se ha visto expuesta a un mayor número de ataques, que demuestran que su sistema no es infranqueable, no obstante en la mayoría de los casos han demostrado una pronta respuesta y siguen siendo sistemas sobre Unix que es una base muy sólida, pero nada de esto vale si el usuario final instala programas de fuentes no confiables o hace caso a todos los *adds* de las páginas de descarga piratas o similares.

LINUX

Introducción

Independientemente de la buena fama respecto a seguridad informática que se le ha atribuído a Linux desde su nacimiento (y su gran crecimiento), por supuesto no es un sistema infranqueable (ni mucho menos). A continuación se comentarán algunos de los problemas de seguridad que ha sufrido a lo largo de sus 25 años.

Vulnerabilidades

GHOST

Descubierto y parcheado por investigadores de la empresa de seguridad Qualys en 2013. Este bug afecta a todos los Linux construidos con **glib-2.2**.

Este fallo de seguridad podía explotarse a través de la función *gethostbyname* de **glibc** la cual se utiliza para llamar a un nodo utilizando el archivo /etc/hosts o mediante DNS.
Sería suficiente con que el atacante fuese capaz de provocar un desbordamiento de memoria usando un nombre de host inválido sobre el servicio de DNS.

Hoy en día todos los SSOO Linux tienen el parche (si sus usuarios lo han actualizado) que palia este bug.

ACCESO ROOT

En diciembre de 2015 se descubrió que pulsando 28 veces la tecla de retroceso se iniciaba un "Grub Rescue Shell" desde el que se podía acceder al equipo sin usar ninguna clave. Un año después de este "bug" vuelve a aparecer una vulnerabilidad curiosa: si mantenemos pulsada la tecla Enter durante 70 segundos tenemos a acceso de root en dicho sistema.

La solución a esta última vulnerabilidad, radica en escribir en consola el siguiente comando para modificar el archivo de configuración de Cryptsetup (responsable del error): ***sed -i 's/GRUBCMDLINELINUXDEFAULT="/GRUBCMDLINELINUXDEFAULT="panic=5 /' /etc/default/grub grub-install***

DIRTY COW

Considerada como la vulnerabilidad más longeva y, posiblemente, la más "mediática", Dirty COW tiene una vida de 11 años; provocada por problemas en el sistema de memoria del kernel al realizar ciertas operaciones de memoria (Copy On Write). El principal problema de la existencia de esta vulnerabilidad es que permite una escalada de privilegios a usuarios locales (con permisos limitados) hasta conseguir privilegios de root.

Todavía sigue habiendo equipos que no han podido superar este problema (debido a que no se han publicado parches que implementen una solución), pero para aquellos que pueden, con actualizar el sistema y reiniciar el servidor, sería suficiente: ***sudo apt-get update && sudo apt-get dist-upgrade***

LLAVERO KERNEL LINUX

En este caso, las funciones Add_key y request_key keyctl han sido las afectadas (desde 2012 a principios de 2016). Estas funciones pertenecen al llavero del kernel de Linux y son las encargadas de permitir la ejecución de código con permisos de kernel para añadir y recuperar contraseñas, por ello (y por los cuatro años de duración) podemos considerarlo como un fallo muy grave, puesto que también habría la posibilidad de ejecutar código remoto con permisos de kernel

La solución es simple ya que con un pequeño parche se tapa la vulnerabilidad, excepto para usuarios de Android con Smartphones antiguos que no pueden actualizar su sistema. Para Linux en Pc, los comandos a seguir serían:

- ***sudo apt update***
- ***sudo apt upgrade***
- ***sudo reboot***

TCP

TCP sirve para empaquetar e intercambiar datos entre diferentes ordenadores a través de internet, asegurando que la integridad de los mismos permanezca intacta. La vulnerabilidad CVE-2016-5696 que se da en kernels con versión 3.6 o superior permite inyectar código malicioso permitiendo predecir los números de secuencia TCP utilizados para la identificación entre partes.

Se han propuesto varias medidas temporales para evitar cualquier posible ataque, como aumentar el ratio ack en el archivo de configuración de ***sysctl,*** aunque todavía no se conoce solución definitiva ni parche que solucione dicha vulnerabilidad.

Evolución y conclusiones del sistema.

Podemos considerar a Linux como un SO seguro y con pocas vulnerabilidades graves a lo largo de su historia, contando con la ventaja de que sus parches suelen conseguirse rápida y fácilmente evitando riesgos. Teniendo en cuenta que es un Sistema Operativo en el cual el usuario puede manejar con relativa facilidad sus configuraciones, podemos adaptar nuestra seguridad de manera relativamente sencilla en cuestión de modificaciones de archivos de configuración.

WINDOWS

Introducción

Para encontrar el primer sistema operativo de Microsoft hay que remontarse a 1985, año en el que ve la luz MS-DOS. Desde entonces, se han sucedido diversas versiones del sistema, guiadas por la visión de diferentes directivos, que con su grano de arena han convertido a Windows en el sistema operativo de referencia para cualquier ordenador personal.

Vulnerabilidades

EJECUCIÓN DE CÓDIGO SIN AUTORIZACIÓN

Este fallo de seguridad, que afectaba a casi todas las versiones del sistema operativo desde Windows Server 2003 en adelante, permitía la ejecución remota de código en caso de que el atacante enviase paquetes con modificaciones concretas a un servidor Windows. Esta falla se considera "crítica" debido a que pertenecía a la biblioteca Schannel, capa que soporta la encriptación y la autenticación de Windows.

Como solución a esta vulnerabilidad, fue lanzada la actualización de seguridad MS14-066.

REDIRECCIÓN A SMB

LLamada redirección a SMB debido al protocolo Server Message Block implicado, esta falla de seguridad permitía robar contraseñas de cualquier versión de Windows (tabletas, ordenadores,servidores). 31 empresas se vieron afectadas directamente con algunos de sus programas (Adobe Reader, iTunes, QuickTime, Internet Explorer, Norton, Windows Player, Excel, etcétera). Microsoft conocía dicha vulnerabilidad desde 1997 y afectaba a Internet Explorer. Originalmente permitía robar los datos de usuario a través del protocolo SMB. El proceso consistía en que al cambiar el protocolo HTTP habitual de cualquier dirección por la palabra "file" se lograba que el sistema se autenticara mediante SMB con la *IP*

1.1.1.1, por lo que para robar la información personal sólo era necesario conseguir que la víctima abriese algún links envenenado.

A día de hoy no hay una solución oficial óptima por lo que para evitar riesgos se propone el bloqueo del tráfico saliente en los puertos 139 y 445 correspondientes al protocolo SMB para así impedir conexiones no deseadas volviendo el robo de datos casi imposible.

REMOTE CODE EXECUTION FONT DRIVER

Esta vulnerabilidad crítica es un problema a nivel de código y sucedía cuando la biblioteca "Windows Adobe Type Manager" no podía procesar las fuentes personalizadas de OpenType provocando que atacantes puedan tomar control completo del sistema afectado.

Las dos formas de tomar dicho control serían:

- Convencer al usuario de abrir un documento malicioso.
- Convencer al usuario de entrar a un sitio web que utilice tipografías de OpenType.

Si el atacante lograse que se diese alguna de las anteriores, ganaría pleno acceso para instalar programas, ver, cambiar y borrar información, o crear nuevos usuarios con permisos de administrador.

Esta falla fue solventada en el parche de seguridad MS15-078.

KERNEL & FLASH

Esta vulnerabilidad surge por un bug en el kernel de Windows que, aprovechando otro bug en Adobe Flash, permite eludir la seguridad del sistema. Esta falla fue expuesta públicamente por Google declarando que su navegador "Chrome" bloqueaba esta vulnerabilidad. Según la publicación de Google la falla puede dispararse a través de una llamada a win32k.sys, método NtSetWindowsLongPtr().

La vulnerabilidad fue solventada por Adobe con una nueva versión de Flash que vió la luz el día 26 de Octubre de 2016, justo 5 días después de la publicación de Google.

Shift + F10 ROOT

Este bug surge de una de las últimas actualizaciones de Windows, con la que podemos obtener privilegios de administrador con el uso de una simple combinación de teclas. Una vez se procede a la actualización de Windows Update, bastaría con reiniciar el sistema y acto seguido, en el proceso de inicio, pulsar las teclas Shift+F10 para conseguir acceso a cmd con permisos de administrador y, por ende, control total del dispositivo.

Actualmente no hay una solución oficial del bug, pero debido a la gravedad añadida es de suponer que Microsoft no tardará demasiado en parchearlo.

Evolución y conclusiones del sistema.

Sobre Microsoft destacar la gran problemática de desarrollar nuevas versiones de su sistema operativo sin solventar aquellos ‘bugs’ recurrentes que exponen el sistema, aún sabiendo de su existencia y gravedad.

BIBLIOGRAFÍA

Mac

- ➔ Historia del malware en OS X
- ➔ ¡Sorpresa!, OS X, iOS y Linux con más bugs que Windows
- ➔ Dropbox NO es seguro: toma el control de tu Mac sin permiso
- ➔ Vulnerabilidad de Mac OS X permite eludir fácilmente su seguridad

Linux

- ➔ TOP 10 DE VULNERABILIDADES WINDOWS Y LINUX SEGÚN EL SANS
- ➔ Una vulnerabilidad puede darte acceso root en Linux pulsando Intro durante 70 segundos
- ➔ Dirty Cow. Vulnerabilidad en Linux permite conseguir privilegios de …
- ➔ Falla Kernel 2012 Android
- ➔ Descubierta grave vulnerabilidad de TCP en Linux

Windows

- ➔ http://www.elconfidencial.com/tecnologia/2015-04-15/windows-10-vulnerabilidad-smb_759720/
- ➔ http://www.eleconomista.es/tecnologia/noticias/6236693/11/14/Microsoft-descubre-una-vulnerabilidad-critica-en-Windows-e-insta-a-actualizar.html
- ➔ http://www.genbeta.com/actualidad/google-indigna-a-microsoft-tras-desvelar-una-importante-vulnerabilidad-para-windows-10
- ➔ https://www.cnet.com/es/noticias/microsoft-parche-vulnerabilidad-afecta-windows-10/
- ➔ http://www.genbeta.com/seguridad/un-fallo-de-seguridad-en-windows-10-permite-obtener-privilegios-de-admin-pulsando-solo-dos-teclas