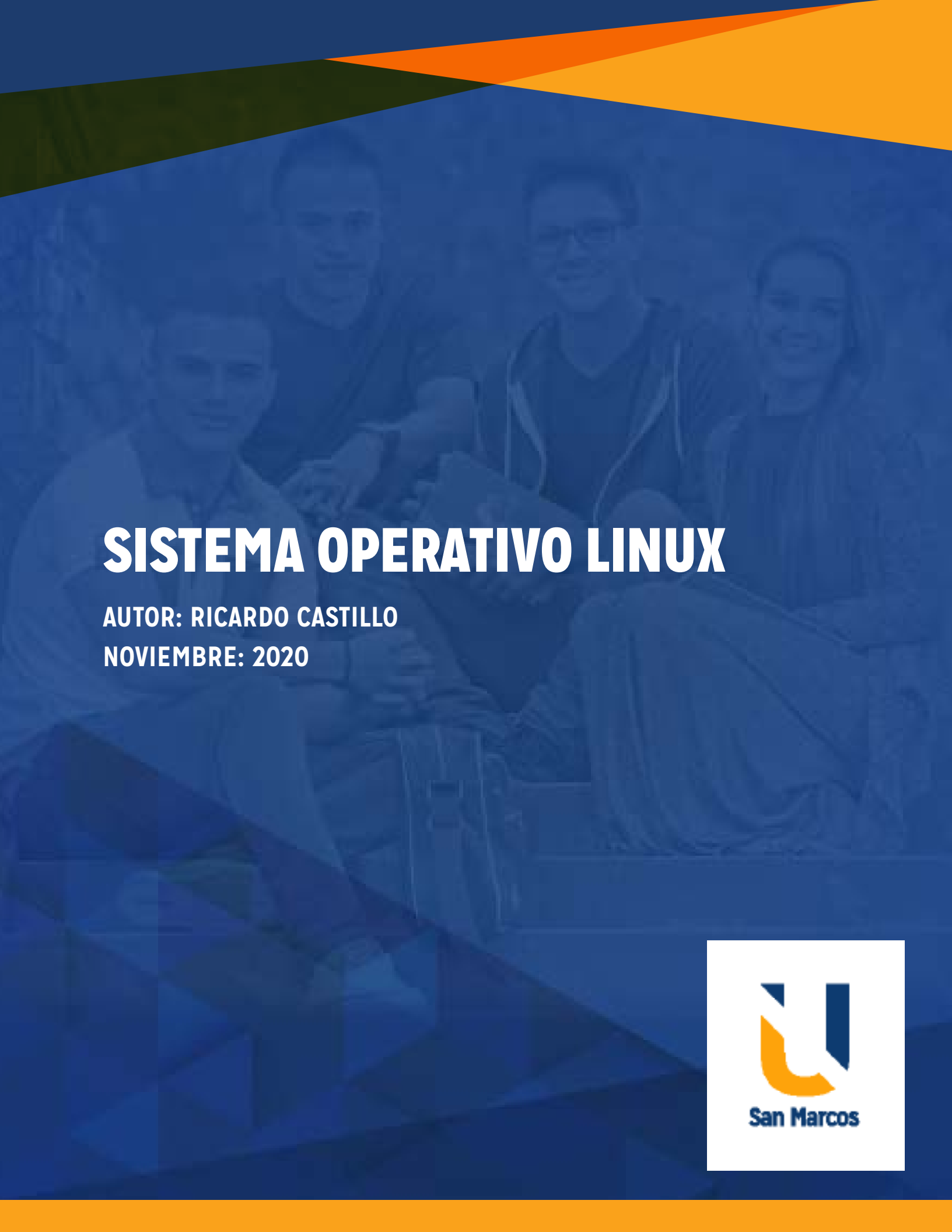

SISTEMA OPERATIVO LINUX

AUTOR: RICARDO CASTILLO

NOVIEMBRE: 2020

San Marcos

Introducción

Ciertamente los sistemas operativos basados en Linux son muchísimo más robustos y seguros comparados con sistemas privativos. Sin embargo, no significa que no hay que preocuparse por virus o malware en Linux. Independientemente del sabor y el tamaño de la instalación de Linux que se esté ejecutando, ya sea un solo escritorio o una granja de servidores, es fundamental prestar atención a la seguridad.

Probablemente, algún usuario principiante se estará preguntado, ¿Qué es un malware? Pues un Malware, o software malicioso, es cualquier programa o archivo que resulte dañino para un computador. Para conocer más sobre este tema es que a continuación se hará referencia a los aspectos relevantes sobre Linux y las vulnerabilidades que pueda presentar.

Contenido

Introducción 1
¿Qué es Linux? 3
Amenazas para Linux 3
¿Cuáles son las que más se propagan y de qué tipo son? 3
Escalamiento de privilegios en FreeBSD 3
Vulnerabilidades en el Kernel de Linux 4
Ubuntu con una vulnerabilidad de severidad alta 4
Otras vulnerabilidades usadas 4
Sophos Antivirus para Linux 5
Conclusiones y recomendaciones 6
Referencias bibliográficas 6

¿Qué es Linux?

Linux es un sistema operativo (SO) de código abierto y una plataforma de infraestructura de TI. Originalmente, fue concebido y creado como un pasatiempo por Linus Torvalds. Mientras estaba en la universidad, Linus intentó crear una versión de open source, alternativa y gratuita, del sistema operativo MINIX, que se basaba en los principios y el diseño de Unix. Desde entonces, ese pasatiempo se ha convertido en el SO con la base más grande de usuarios, es el SO más usado en servidores de Internet disponibles públicamente y en el único SO usado en las 500 principales supercomputadoras más rápidas.

Linux puede servir como base para casi todos los tipos de iniciativas de TI, incluidos los contenedores, las aplicaciones nativas de la nube y la seguridad. Es la base de algunos de los sectores y empresas más grandes del mundo, desde los sitios web que comparten conocimientos, como Wikipedia y New York Stock Exchange, hasta los dispositivos móviles que utilizan Android (que es una distribución de uso específico del kernel de Linux con software complementario). Con el transcurso de los años, Linux se ha convertido en el estándar "de facto" para las cargas de trabajo fundamentales, de alta disponibilidad y confiabilidad en los centros de datos y las implementaciones de la nube. Tiene varios casos prácticos, distribuciones, sistemas objetivo, dispositivos y capacidades, y todo se basa en las necesidades del usuario y las cargas de trabajo.

Amenazas para Linux

¿Cuáles son las que más se propagan y de qué tipo son?

Escalamiento de privilegios en FreeBSD

En primer lugar, se encuentra la detección del exploit para aprovechar la vulnerabilidad CVE-2013-2171, que permite hacer un escalamiento de privilegios en FreeBSD. Este sistema operativo quizá no sea el más popular cuando se trata de computadoras de escritorio, por su compatibilidad de hardware, pero sí es bastante utilizado cuando se trata de servidores.

Si esta vulnerabilidad reportada en junio de 2013 es explotada, puede permitir la modificación no autorizada de un archivo arbitrario al que el atacante tenga acceso de

lectura. Esto, dependiendo del archivo y la naturaleza de las modificaciones, puede dar lugar a un escalamiento de privilegios.

Es importante aclarar que para para aprovechar esta vulnerabilidad, basta con que el atacante pueda ejecutar código arbitrario con privilegios de usuario en el sistema de destino. La corrección de esta vulnerabilidad está disponible a partir de la versión 9.1 del sistema operativo.

Vulnerabilidades en el Kernel de Linux

En segundo lugar, aparece la vulnerabilidad CVE-2014-3153, la cual está asociada con un problema en las llamadas futex. Si esta vulnerabilidad es aprovechada permitiría a un usuario local y sin privilegios bloquear el kernel (lo que resultaría en la denegación de servicio) o incluso escalar privilegios en el sistema.
Al ser una vulnerabilidad en la versión 3.14.5 del Kernel de Linux, varias distribuciones se vieron afectadas. Sin embargo, la mayoría fueron corrigiéndola hacia mediados de 2014, por lo que bastaría con actualizar para corregirla.

Ubuntu con una vulnerabilidad de severidad alta

La vulnerabilidad CVE-2015-1328 está asociada con la funcionalidad OverlayFS, utilizada para unir directorios o sistemas de archivos. Esta vulnerabilidad está presente en las versiones Ubuntu 12.04/14.04/14.10/15.04.
Como no se comprueban correctamente los permisos para la creación de archivos, los usuarios locales pueden obtener acceso root al sistema.

Otras vulnerabilidades usadas

Mientras en sistemas operativos Windows hablamos de ransomware y botnets, en Linux lo que más encontramos son códigos maliciosos relacionados con la explotación de vulnerabilidades, incluso algunas con más de 10 años como CVE-2003-0127, que se encuentra dentro de los 20 códigos maliciosos más detectados en plataformas Linux.

Sophos Antivirus para Linux

Sophos es una compañía antivirus comercial que ofrece una utilidad gratuita de exploración. Esta herramienta utiliza un motor de exploración con el cual identifica, aísla y elimina troyanos, virus y una variedad de tipos de malware en Linux.

Más importante aún, el programa también detecta, bloquea y elimina malware de Windows, Mac y Android, lo que lo convierte en una excelente opción para los servidores de archivos. Incluso funciona con servidores web, servidores NFS o viejos servidores de archivos FTP. Si tienes un sistema Linux que sirve archivos, es fundamental que los escanee para asegurarse de que no se haya convertido en un punto de distribución de malware.

Conclusiones y recomendaciones

En conclusión, todos los sistemas operativos de una u otra manera pueden verse afectados por hackers, lo importante es havcer un estudiosobre cual posee menos vulnerabilidades. Un punto a favor del sistema operativo Linux es que todas las vulnerabilidades están en distribuciones para las cuales ya existe una actualización que corrija el problema. Así que es hora de verificar qué versión del sistema operativo se está utilizando y, si se está dentro de las versiones vulnerables, planear la mejor manera de hacer la actualización y evitarse complicaciones en el futuro.

Referencias bibliográficas

- Ayuda Linux (2018) Malware en Linux: ¿Qué son? ¿Cómo analizarlos y eliminarlos? Recuperado de: https://ayudalinux.com/malware-en-linux-analizarlos-eliminarlos/

- ESET (2017) Amenazas para Linux: ¿cuáles son las que más se propagan y de qué tipo son? Recuperado de: https://www.welivesecurity.com/la-es/2017/07/25/amenazas-para-linux-mas-se-propagan/

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica