

SEGURIDAD DE LA INFORMACIÓN Redes, informática y sistemas de información

Autor: Javier Areitio Bertolín
Editorial: Paraninfo
Año 2008 – 592 páginas
ISBN: 8497325028 **EAN:** 9788497325028
www.thomsonparaninfo.com

Por fin ha visto la luz, editada por Paraninfo, la obra –llamada a convertirse en un clásico de la especialidad– de uno de los grandes expertos en seguridad de la información y gran profesor con que contamos en España, el Dr. **Javier Areitio Bertolín**, Catedrático de la Universidad de Deusto, Director del Grupo de Investigación de Redes y Sistemas, Director del Máster Oficial de Seguridad de la Información de esta Universidad, y responsable desde su creación de la sección Laboratorio de la revista SIC.

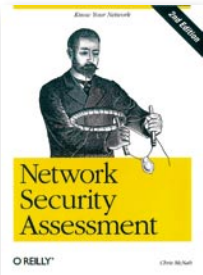
El volumen –que será en un futuro glosado en profundidad– permite conocer a fondo, de forma amena, desde la doble perspectiva teórica

y práctica, los fundamentos y los aspectos más relevantes y apasionantes de la Seguridad de la Información, desde la perspectiva de la protección tanto de los sistemas de información como de las redes y de los computadores.

Se trata de un continuo desafío, ya que –como es sabido– más que un problema únicamente tecnológico, constituye hoy en día un elemento clave que posibilita los negocios y permite que las organizaciones puedan llevar a cabo sus objetivos corporativos. Aunque controlar y dominar los secretos de la seguridad de la información puede parecer reservado sólo a unos pocos, el objetivo de este libro es proporcionar

un referente actual de las cuestiones clave desde la perspectiva teórica-práctica de este fascinante mundo. No sólo se busca la asimilación de la teoría a través de ejemplos, sino que además se implica al lector en una dinámica rica en actividades y retos, tanto cualitativos y cuantitativos como de representación gráfica.

El sumario del libro se compone de los siguientes capítulos: **Prólogo** 1. **Fundamentos de seguridad de la información** 2. **Análisis y gestión de riesgos de seguridad** 3. **Control de acceso: Autenticación, autorización y cumplimiento** 4. **Análisis de ataques a los sistemas de información** 5. **Sistemas de gestión de seguridad de la información. Métricas, cuadros de mando y criterios de evaluación** 6. **Planificación de contingencias y continuidad de negocios** 7. **Cumplimiento con las leyes. Privacidad y anonimato. Servicios de investigación y responsabilidad** 8. **Tecnologías de seguridad** 9. **Análisis y síntesis de funcionalidades criptográficas simétricas** 10. **Análisis y síntesis de funcionalidades criptográficas asimétricas**. El volumen se completa con la correspondiente **Bibliografía** y un **Índice terminológico**. ■



NETWORK SECURITY ASSESSMENT

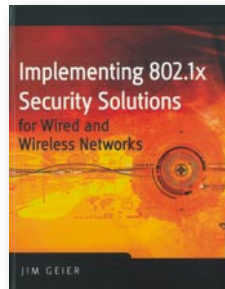
Autor: Chris McNab
Editorial: O'Reilly
Año 2008 – 478 páginas
ISBN: 978-0-596-51030-5
www.oreilly.com

La evaluación es habitualmente uno de los primeros pasos que una organización efectúa para empezar a gestionar los riesgos de la información, ya que sólo valorando la red de la misma forma en que un atacante lo haría, se puede gestionar el riesgo de un modo proactivo. Por este motivo, el autor de la obra glosada, **Chris McNab**, sostiene que la mejor manera de averiguar si una red es segura o no es atacándola, y en *Network Security Assessment* muestra la manera en que un atacante rastrea las redes en busca de componentes vulnerables, desde el nivel de la red hasta el nivel de las aplicaciones.

La obra también proporciona los modelos de simulacro de penetración utilizados para proteger las redes gubernamentales, militares y comerciales, lo que permite al lector perfeccionar y

reutilizar dichos modelos para desarrollar redes más resistentes contra los ataques; y adicionalmente, esta segunda edición ha sido actualizada con las últimas técnicas de *hacking*, con el fin de que el lector aprenda a crear estrategias defensivas contra categorías de ataques completas, que sirvan para proteger sus redes no solo ahora, sino también en el futuro.

Es importante señalar que el texto solo trata un aspecto muy concreto de la seguridad de la información, que es la evaluación de la seguridad de una red basada en protocolos de Internet (IP). Por tanto, su lectura es fundamentalmente adecuada para administradores de redes, consultores de seguridad, y otros técnicos familiarizados con sistemas operativos basados en administración Unix e IP, como Linux o Solaris. ■



IMPLEMENTING 802.1X SECURITY SOLUTIONS FOR WIRED AND WIRELESS NETWORKS

Autor: Jim Geier
Editorial: Wiley
Año 2008 – 330 páginas
ISBN: 978-0-470-16860-8
www.wiley.com

El autor del presente libro parte de la base de que la autenticación basada en el puerto 802.1X resulta más difícil de comprender y desarrollar de lo que comúnmente se piensa, y prueba de ello es que la mayoría de los administradores e ingenieros tienen dificultades para conseguir que estos sistemas funcionen correctamente, debido, sobre todo, a la escasez de conocimiento y de experiencia en estas soluciones.

En este sentido, la obra de **Jim Geier** constituye un interesante manual para aquellos administradores de sistemas e ingenieros de redes involucrados en el desarrollo de sistemas de información seguros, pues las explicaciones en profundidad de los protocolos de autenticación y los numerosos consejos que contiene el texto, resultan de gran utilidad a la hora de desarrollar y mantener sistemas basados en el estándar 802.1X.

En concreto, el volumen proporciona a través de nueve capítulos una visión general de los conceptos de autenticación basada en puerto y de arquitectura de red; examina los protocolos EAPOL, Radius y los métodos EAP; profundiza en las operaciones y estructura de paquetes del protocolo 802.1X; evalúa soluciones de seguridad completas basadas en 802.1X para distintas necesidades; expone qué partes son necesarias para construir un sistema completo de control de acceso a la red; y, en definitiva, señala paso a paso cómo establecer con éxito soluciones de seguridad basadas en 802.1X y hacer que funcionen.

Cabe finalizar señalando que el volumen incorpora como apéndice una exhaustiva descripción del RFC 3748, conocido como EAP (*Extensible Authentication Protocol*) y se completa con un útil glosario. ■