# Internal Hacking y contramedidas en entorno Windows : Pirateo interno, medidas de protección, desarrollo de herramientas (2º edición) /

Ediciones ENI,
2018

Libros electrónicos | Documentos electrónicos ENI

Monografía

Este libro se dirige a los Administradores de Sistemas Windows, a los Responsables de Seguridad y a los Desarrolladores entusiastas con la seguridad informática. Tiene por objetivo el aprender a conocer mejor los riesgos de ataques internos, al alcance de usuarios simples, y por lo tanto favorecer la puesta en marcha de contramedidas que, obligatoriamente, aumentarán la seguridad frente a ataques externos. En efecto, muchos estudios muestran que se puede atactar fácilmente la infraestructura informática de una empresa desde el interior, habiendo un claro aumento de este tipo de incidentes. La realidad es así, regularmente se utilizan técnicas de hacking para estos fines. El autor describe por ejemplo cómo convertirse en administrador en un puesto de trabajo o en un servidor (cuando se es un usuario con pocos o ningún permiso), cómo apropiarse de una contraseña, coger el control remoto de un puesto, cómo ejecutar una aplicación trampa, sobrepasar las restricciones software, crear un cryptoware... Los medios utilizados se componen de recursos internos así como de los programas estrellas del pirateo en entorno Windows. Se llevará también al lector a crear sus propias herramientas para escapar mejor al control de los antivirus y rodear las medidas clásicas de protección configuradas. Frente a estos riesgos, el autor describe las contramedidas técnicas a poner en marcha como las estrategias de grupo, los certificados, los smartcards virtuales, la autentificación OTP… Inicia también al lector a una buena gestión de los sistemas para darle los medios para proteger mejor sus sistemas de información. Le guiará en la puesta en marcha de un protocolo de seguridad y la adopción de reglas simples para incrementar la resistencia de su infraestructura. Casi todos los cambios preconizados y configurados son igualmente beneficiosos frente a las amenazas externas y contribuyen por lo tanto a un retorno de la inversión rápido y eficaz. Se pueden descargar elementos adicionales en el sitio web www.ediciones-eni.com. Los capítulos del libro: Prólogo - Introducción - Búsqueda de información - Tomar el rol de administrador o de sistema - Encriptado y CryptoLocker - Extraer, romper, cambiar una contraseña - Desarrollar sus propias herramientas de hacking - Hacer ejecutar sus aplicaciones trampa - Superar las restricciones de software - Tomar el control remotamente - Guardar una puerta abierta - Esconderse y eliminar sus huellas - Las contramedidas técnicas - La gestión de los sistemas de información

**Título:** Internal Hacking y contramedidas en entorno Windows Pirateo interno, medidas de protección, desarrollo de herramientas (2º edición) Philippe KAPFER

**Editorial:** Barcelona Ediciones ENI 2018

**Descripción física:** 570 pages

**Tipo Audiovisual:** anti virus antivirus hacker LNEPT2INTH pirateo protección libro seguridad

**Mención de serie:** EPSILON

**Nota general:** Autor: KAPFER, Philippe Edición del 6 February 2018

**Restricciones de acceso:** El acceso al documento requiere autenticación con la cuenta del campus virtual UPSA

**Detalles del sistema:** Para la consulta del documento es necesario introducir un seudónimo y una contraseña (opcional). Puede escoger el seudónimo y la contraseña que desee. Su único objetivo es reconocerle la próxima vez que consulte la biblioteca Online ENI, de modo que conserve sus favoritos, marcapáginas y anotaciones. No permite la descarga ni la impresión del contenido

**ISBN:** 9782409012990 versión digital online) 9782409012969 versión impresa)

**Entidades:** Ediciones ENI (Cornellà de Llobregat, España) ENI Biblioteca Online (Servicio en linea)