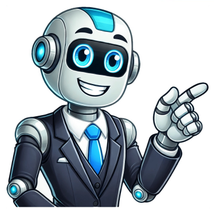
Click Here



El libro del hacker 2018 pdf

por Maria Angeles Caballero VelascoResumen del libro El Libro Del Hacker (ed. 2018) en PDF, Docx, ePub y AZWDía a día nos encontramos poco a poco más y mucho más rodeados de tecnología. La manera en que nos avisamos y compartimos datos en internet cambió radicalmente en las últimas décadas. Es evidente el valor que nos contribuye la tecnología a los humanos, pero asimismo es cierto que fué acompañada de un aumento en los riesgos de seguridad. Las clases pésimos renuevan regularmente los ciberataques y las ciberarmas, lo que hace que los ciudadanos de caminando como las compañías deban superar y saber las mucho más recientes noticias de ciberseguridad y hacking. En esta edición novedosa 2018, los autores nos muestran desde los conceptos básicos de seguridad y técnicas de hacking hasta entendimientos avanzados en ciberseguridad, como las mucho más recientes técnicas de ataque. Nos se dan cuenta los desafíos y peligros de la identidad digital, criptografía y firma electrónica, técnicas de intrusión, hacking web, exploiting, etcétera Asimismo van a abordar los sistemas tecnológicos industriales y los riesgos y asaltos socios. Observaremos la administración de crisis y wargaming, y finalmente, introducirán al lector en los conceptos de ciberarmas y ciberamenazas que desarrollan tanto los ciberdelincuentes y mafias organizadas como los gobiernos y países: la guerra treinta.Ficha técnica de El Libro Del Hacker (ed. 2018) Titulo del libro "El Libro Del Hacker (ed. 2018)" Registro ISBN ° 9788441539648 Publicado por Editorial Anaya Multimedia Escrito por Maria Angeles Caballero Velasco Publicado el Año 2017 Origen del Libro España Idioma de publicación Castellano Tipo de Encuadernación original Tapa Blanda Cada vez es más la tecnología que nos rodea. Y aunque es indiscutible el valor que nos aporta, también es cierto que esta evolución tecnológica ha ido acompañada de un incremento en los ciberriesgos. Los ciberdelincuentes renuevan constantemente las tácticas, técnicas y procedimientos de los ciberataques, lo que hace que tanto los ciudadanos de a pie como las empresas tengan que evolucionar y conocer las últimas novedades de ciberseguridad y 'hacking'.En esta nueva edición de 'El libro del hacker' os mostraremos desde los conceptos básicos de seguridad y técnicas de 'hacking' hasta conocimientos avanzados, así como las más novedosas técnicas de ataque. Conoceremos las principales ciberamenazas y actores asociados. Hablaremos de ciberguerra y ciberespionaje. Abordaremos los retos y riesgos de 'Cloud', los datos, identidad digital, criptográfica y 'blockchain'. Veremos técnicas de intrusión, 'hacking web' y microservicios, 'exploiting', metodologías de 'pentesting' y análisis forense. También abordaremos los sistemas tecnológicos industriales e IoT, los riesgos y ataques asociados.Además, porque es interesante conocerlo, dedicamos un capítulo a indagar, desde un punto de vista psicológico y sociológico, la mente del cibercriminal, la forma de pensar, perfiles y tácticas de influencia, de manera que podamos entender mejor las motivaciones de estos profesionales del bien (hackers éticos) como del mal (ciberdelincuentes). Leyendo este libro aprenderás desde conceptos esenciales de seguridad informática hasta aspectos avanzados relacionados con la ciberseguridad. Los autores de "El libro del hacker" son María Ángeles Caballero Velasco y Diego Cilleros Serrano. El libro ha sido publicado por la editorial ANAYA MULTIMEDIA. Descripción del libro Este libro es ideal para todos aquellos que quieran aprender seguridad informática sin tener conocimientos previos. Su lectura es muy amena y, aunque con él no llegarás a convertirte en un experto, sí te introducirá en el conocimiento de técnicas de hacking, criptografía, exploiting, etc. Puedes ver más información del libro y consultar su precio en Amazon Detalle del libro Ver Índice 1. El mundo digital es inseguroIdentificando amenazas en la redTerminología básica de hackingConceptos y enfoquesLa cadena del ataqueTipos de ciberataques 2. Diseño seguro de redesConceptos de red y comunicacionesLa seguridad en la red de datos 3. Criptografía y firma digital Definición y tipos de sistemas criptográficosCriptografía de clave asimétricaAlgoritmos de hashingFirma digital y certificadosAplicacionesAtaques 4. Retos de la identidad digitalLa nueva identidad, identidad en la redIdentidad como autenticaciónIdentidad personalIdentidad corporativaRiesgos de la identidad digital 5. Protección de la información digitalFuentes de información públicaCompartición de ciberinformaciónHuella en Internet 6. Test de intrusiónConceptosMetodologíasInformation GatheringAnálisis de vulnerabilidadesTrabajar con exploitsEscalado de privilegiosAtaques a credencialesAnálisis de tráfico y túneles 7. Hacking Web y seguridad en microserviciosOWASP Top10Fuzzing Web y búsqueda de informaciónXSS y SQL InjectionEjecución de comandosFuga de información 8. ExploitingConceptosBuffer OverflowsEncoding 9. Hacking WiFi y VoIPWireless Wi-FiVoIP 10. Análisis forenseCiencia forenseEvidencia digitalCasos en los que es necesario el análisis forenseEtapas en la investigaciónCSIRTHerramientas forensesCaso práctico 11. Mundo industrial e IoTIndustria 4.0ArquitecturasRiesgos de seguridadLa seguridad como reto en IoT 12. Gestión de crisis y wargamingCiberamenazas y guerra 3.0IntroducciónGuerra 3.0AmenazasAtaques dirigidos o APTsMalware "avanzado" Fraude online Cada día estamos más y más rodeados de tecnología. La forma en que nos comunicamos y compartimos datos en la red ha cambiado radicalmente en las últimas décadas. Es indiscutible el valor que nos aporta la tecnología a los seres humanos, pero también es cierto que ha ido acompañada de un incremento en los riesgos de seguridad. Los tipos malos renuevan constantemente los ciberataques y las ciberarmas, lo que hace que tanto los ciudadanos de a pie como las empresas tengan que evolucionar y conocer las últimas novedades de ciberseguridad y hacking. En esta nueva edición 2018, los autores nos presentan desde los conceptos básicos de seguridad y técnicas de hacking hasta conocimientos avanzados en ciberseguridad, así como las más novedosas técnicas de ataque. Nos descubren los retos y riesgos de la identidad digital, criptografía y firma electrónica, técnicas de intrusión, hacking web, exploiting, etc. También abordarán los sistemas tecnológicos industriales y los riesgos y ataques asociados. Veremos la gestión de crisis y wargaming, y por último, introducirán al lector en los conceptos de ciberarmas y ciberamenazas que desarrollan tanto los ciberdelincuentes y mafias organizadas como los gobiernos y países: la guerra 3.0. Otros compraron Libros Informática Informática práctica Seguridad infórmatica ANAYA MULTIMEDIA - 9788441539648 Informática práctica Seguridad infórmatica Cada día estamos más y más rodeados de tecnología. La forma en que nos comunicamos y compartimos datos en la red ha cambiado radicalmente en las últimas décadas. Es indiscutible el valor que nos aporta la tecnología a los seres humanos, pero también es cierto que ha ido acompañada de un incremento en los riesgos de seguridad. Los tipos malos renuevan constantemente los ciberataques y las ciberarmas, lo que hace que tanto los ciudadanos de a pie como las empresas tengan que evolucionar y conocer las últimas novedades de ciberseguridad y hacking. En esta nueva edición 2018, los autores nos presentan desde los conceptos básicos de seguridad y técnicas de hacking hasta conocimientos avanzados en ciberseguridad, así como las más novedosas técnicas de ataque. Nos descubren los retos y riesgos de la identidad digital, criptografía y firma electrónica, técnicas de intrusión, hacking web, exploiting, etc. También abordarán los sistemas tecnológicos industriales y los riesgos y ataques asociados. Veremos la gestión de crisis y wargaming, y por último, introducirán al lector en los conceptos de ciberarmas y ciberamenazas que desarrollan tanto los ciberdelincuentes y mafias organizadas como los gobiernos y países: la guerra 3.0. Ver más Fecha de lanzamiento: 16/11/2017 Información otros vendedores María Ángeles Caballero Velasco cuenta con más de diez años de experiencia en el sector de la ciberseguridad. Actualmente es 'Head of Cybersecurity' para una de las principales entidades del Banco Santander en el ámbito de CISO (Chief Information Security Officer). Es ingeniera en Informática Técnica de Gestión y licenciada en Administración y Dirección de Empresas por la Universidad Carlos III de Madrid. También ha cursado el Máster Universitario en Seguridad de las TIC por la UEM y el Máster en Design Thinking por el MIT. Posee múltiples certificaciones, como CISSP, SSCP, CEH o PMP, y tiene numerosas publicaciones en libros, revistas y foros, habiendo publicado siete libros de ciberseguridad hasta la fecha. Ha participado en múltiples seminarios, conferencias y cursos, dado que le entusiasma la concienciación y la formación.Finalmente, su pasión por el comportamiento y la cognición humana le ha llevado a cursar actualmente el Grado de Psicología por la UNED y a certificarse como 'coach' profesional con la escuela americana IPEC. Ver ficha del autor Diego Cilleros Serrano es ingeniero superior de Telecomunicaciones por la Universidad Carlos III de Madrid y estudiante del Grado de Criminología por la Universidad Internacional de La Rioja. Su experiencia profesional ha estado siempre ligada al mundo de las redes de datos y de la ciberseguridad. Trabaja actualmente como gerente senior de ciberseguridad en el área Cyber Risk Services de Deloitte España y es responsable de un equipo cercano a las cien personas dedicado a las arquitecturas de seguridad y a la seguridad 'cloud'. Posee diferentes certificaciones de ciberseguridad que complementan su experiencia, como Offensive Security Certified Professional (OSCP), Certified SCADA Security Architect (CSSA), CISSP, CCSP, CSX y CISA, y algunas relacionadas con AWS y Azure, entre otras. Ha participado en diferentes seminarios y cursos y es coautor de diferentes publicaciones sobre ciberseguridad. Ver ficha del autor ¡Sólo por opinar entras en el sorteo mensual de tres tarjetas regalo valoradas en 20€*! Envío gratis a partir de 19.0 € Recogida en librería gratis Devoluciones gratis hasta 14 días Recibe nuestras novedades en libros en tu email © 2025 Casa del Libro. Todos los derechos reservados. v.4.12.27 Ficha realizada por: Selin Explicación exhaustiva de los procedimientos de defensa ante los ciberataques en una edición actualizada que recoge todas las novedades hasta el momento de su publicación. Este es un libro para tomárselo muy en serio, aunque el lector tenga sobrada experiencia informática, porque así podrá saber hasta qué punto está al día en este mundo digital en continua evolución. Y si es un usuario normal, mucho más todavía. Por una parte, es muy importante conocer cuáles podrían ser nuestras vulnerabilidades ante un ciberataque; por otra, seguro que hay mucho para aprender dentro de sus páginas. Porque lo bueno de este libro es que además de una gran cantidad de información y de descripciones muy claras, explica paso a paso cada proceso, que el lector podrá seguir con sus propias pruebas. La prolija descripción de todas las posibilidades de ataque en internet es, al menos hasta casi ahora mismo, exhaustiva. Y vista desde ambos lados, ya que la mejor manera de desarrollar una buena defensa es conocer cómo podemos ser atacados. Los procedimientos están desarrollados con mucho detalle, con abundantes capturas de pantalla que los muestran de manera gráfica, sobre todo cuando se trata de utilizar programas, para evitar cualquier malentendido. Vale que si el lector está acostumbrado a investigar, lo tendrá fácil, pero muchas veces la usabilidad no es un asunto prioritario y se opta por dejarla de lado incidiendo en la eficacia. "El libro del hacker, edición 2018" es un excelente libro para comprender los entresijos y las características de la ciberseguridad, proponiendo un aprendizaje de los recursos disponibles para que la propia información esté lo mejor salvaguardada posible de los ciberataques. Mi recomendación es leerlo con mucha atención y poner en práctica sus propuestas. Tal vez no seamos un objetivo apetecible, pero eso nunca se sabe hasta que llega el problema y lo mejor será que las defensas nos mantengan protegidos. Selin