Hacking Etico 101

Hacking Etico 101 - Cómo Hackear Profesionalmente en 21 días o Menos!

¿Siente curiosidad sobre cómo realizan pruebas de intrusión los hackers? ¿Ha querido tomar cursos presenciales de hacking ético pero no tiene el tiempo o el dinero para hacerlo?Este libro tiene la respuesta para Usted. Con tan sólo 2 horas de dedicación diaria usted puede convertirse en hacker ético profesional!En él encontrará información paso a paso acerca de cómo actúan los hackers, cuáles son las fases que siguen, qué herramientas usan y cómo hacen para explotar vulnerabilidades en los sistemas informáticos. Aprenderá además cómo escribir un informe profesional y mucho más!El libro tiene un enfoque práctico y ameno e incluye laboratorios detallados con populares sistemas operativos como Windows y Kali Linux 2.0.Tópicos cubiertos:* El círculo del hacking* Tipos de Hacking, modalidades y servicios opcionales* Reconocimiento pasivo y activo* Google hacking, consultas WhoIs y nslookup* Footprinting con Maltego y Sam Spade* Métodos de escaneo y estados de puertos* Escaneo con NMAP* Análisis de vulnerabilidades con NeXpose y OpenVAS* Enumeración de Netbios* Mecanismos de hacking* Frameworks de explotación* Metasploit Framework (msfconsole, web y Armitage)* Ataques de claves* Ataques de malware* Ataques DoS* Hacking de Windows con Kali Linux y Metasploit* Hacking inalámbrico con Aircrack-ng* Captura de claves con sniffers de red* Ataques MITM con Ettercap y Wireshark* Ingeniería social con el Social Engineering Toolkit (SET)* Phishing e inyección de malware con SET* Hacking de Metasploitable Linux con Armitage* Consejos para escribir un buen informe de auditoría* Certificaciones de seguridad informática y hacking relevantesSobre la autora:Karina Astudillo es una consultora de sistemas con más de 20 años de experiencia en tecnologías de información. Es experta en seguridad informática, hacker ético certificado (CEH) y tiene a su haber otras certificaciones en IT como CCNA Security, CCNA Routing & Switching, CCNA Wireless, Cisco Security, Computer Forensics US, HCSA, HCSP, Network Security, Internet Security, SCSA y VmWare VSP.En la actualidad se desenvuelve como Gerente de IT de Elixircorp, empresa consultora de seguridad informática especializada en hacking ético y computación forense.Karina es además docente de la Maestría de Seguridad Informática Aplicada (MSIA) y del Cisco Networking Academy Program (CNAP) de la Escuela Superior Politécnica del Litoral (ESPOL), en donde ha sido instructora desde 1996.

Hacking Etico 101

Come hackeare professionalmente in meno di 21 giorni! Comprendere la mente dell’hacker, realizzare ricognizioni, scansioni ed enumerazione, effettuazione di exploit, come scrivere una relazione professionale, e altro ancora! Contenuto: •La cerchia dell'hacking •Tipi di hacking, modalità e servizi opzionale •Riconoscimento passivo e attivo •Google hacking, WhoIs e nslookup •Footprinting con Maltego e Sam Spade •Metodi di scansione e stati della porta •Scansione con NMAP •Analisi della vulnerabilità con Nexpose e OpenVAS •Enumerazione di Netbios •Meccanismi di hacking •Metasploit Framework •Attacchi di chiave •Attacchi di malware •Attacchi DoS •Windows hacking con Kali Linux e Metasploit •Hacking Wireless con Aircrack-ng •Cattura di chiavi con sniffer di rete •Attacchi MITM con Ettercap e Wireshark •Ingegneria sociale con il SET Toolkit •Phishing e iniettando malware con SET •Hacking Metasploitable Linux con Armitage •Suggerimenti per scrivere una buona relazione di controllo •Certificazioni di sicurezza informatica e hacking pertinente

Hacking Etico 101

¿Siente curiosidad sobre cómo realizan pruebas de intrusión los hackers? ¿Ha querido tomar cursos presenciales de hacking ético pero no tiene el tiempo o el dinero para hacerlo?Este libro tiene la respuesta para Usted. Con tan sólo 2 horas de dedicación diaria usted puede convertirse en hacker ético profesional!En él encontrará información paso a paso acerca de cómo actúan los hackers, cuáles son las fases que siguen, qué herramientas usan y cómo hacen para explotar vulnerabilidades en los sistemas informáticos. Aprenderá además cómo escribir un informe profesional y mucho más!El libro tiene un enfoque práctico y ameno e incluye laboratorios detallados con populares sistemas operativos como Windows y Kali Linux (antes Backtrack).Tópicos cubiertos: El círculo del hacking Tipos de Hacking, modalidades y servicios opcionales Reconocimiento pasivo y activo Google hacking, consultas WhoIs y nslookup Footprinting con Maltego y Sam Spade Métodos de escaneo y estados de puertos Escaneo con NMAP Análisis de vulnerabilidades con NeXpose y OpenVAS Enumeración de Netbios Mecanismos de hacking Frameworks de explotación Metasploit Framework (msfconsole, web y Armitage) Ataques de claves Ataques de malware Ataques DoS Hacking de Windows con Kali Linux y Metasploit Hacking inalámbrico con Aircrack-ng Captura de claves con sniffers de red Ataques MITM con Ettercap y Wireshark Ingeniería social con el Social Engineering Toolkit (SET) Phishing e inyección de malware con SET Hacking de Metasploitable Linux con Armitage Consejos para escribir un buen informe de auditoría Certificaciones de seguridad informática y hacking relevantes

Ethical Hacking 101

Curious abot how to perform penetration testings? Have you always wanted to become an ethical hacker but haven't got the time or the money to take expensive workshops? Then this book is for you! With just 2 hours of daily dedication you could be able to start your practice as an ethical hacker, of course as long as you not only read the chapters but perform all the labs included with this book. Table of contents: - Chapter 1 - Introduction to Ethical Hacking - Chapter 2 - Reconnaissance or footprinting - Chapter 3 - Scanning - Chapter 4 - Enumeration - Chapter 5 - Exploitation or hacking - Chapter 6 - Writing the audit report without suffering a mental breakdown - Chapter 7 - Relevant international certifications - Final Recommendations - Please leave us a review - About the author - Glossary of technical terms - Apendix A: Tips for succesful labs - Notes and references

Note: The labs are updated for Kali Linux 2!

Wireless Hacking 101

Wireless Hacking 101 - How to hack wireless networks easily! This book is perfect for computer enthusiasts that want to gain expertise in the interesting world of ethical hacking and that wish to start conducting wireless pentesting. Inside you will find step-by-step instructions about how to exploit WiFi networks using the tools within the known Kali Linux distro as the famous aircrack-ng suite. Topics covered: •Introduction to WiFi Hacking •What is Wardriving •WiFi Hacking Methodology •WiFi Mapping •Attacks to WiFi clients and networks •Defeating MAC control •Attacks to WEP, WPA, and WPA2 •Attacks to WPS •Creating Rogue AP's •MITM attacks to WiFi clients and data capture •Defeating WiFi clients and evading SSL encryption •Kidnapping sessions from WiFi clients •Defensive mechanisms

Reconnaissance 101: Footprinting & Information Gathering

Introducing the \"RECONNAISSANCE 101\" Book Bundle: Unleash Your Ethical Hacking Potential! Are you ready to embark on a thrilling journey into the world of ethical hacking and information gathering? Look no further, because the \"RECONNAISSANCE 101\" Book Bundle is here to equip you with the essential knowledge and skills you need to excel in this exciting field. BOOK 1: RECONNAISSANCE 101: A BEGINNER'S GUIDE TO FOOTPRINTING & INFORMATION GATHERING If you're new to ethical hacking, this beginner's guide is your perfect starting point. Dive into the fundamentals of reconnaissance and information gathering, learning the ropes of footprinting in a clear and approachable manner. Lay a solid foundation for your ethical hacking journey. BOOK 2: MASTERING FOOTPRINTING: ADVANCED INFORMATION GATHERING STRATEGIES FOR ETHICAL HACKERS Ready to take your skills to the next level? In this volume, you'll explore advanced information gathering techniques used by ethical hackers worldwide. Discover how to navigate the digital landscape with precision and uncover hidden insights to enhance your cybersecurity prowess. BOOK 3: THE ETHICAL HACKER'S FIELD GUIDE TO TARGET DATA ACQUISITION Ethical hacking isn't just about collecting data—it's about doing so responsibly and ethically. Book 3 delves into the principles of responsible data acquisition, ensuring you gather valuable information while maintaining the highest ethical standards. Learn how to identify vulnerabilities and strengthen security. BOOK 4: RECONNAISSANCE PRO: THE ULTIMATE HANDBOOK FOR ELITE INFORMATION GATHERERS Are you ready to become an elite information gatherer? This ultimate handbook will elevate your skills to the highest echelons of the field. Uncover the secrets and tactics employed by the best ethical hackers, propelling you into the realm of elite information gatherers. Why Choose the \"RECONNAISSANCE 101\" Book Bundle? · Comprehensive Knowledge: Covering everything from the basics to elite strategies, this bundle provides a complete understanding of reconnaissance and ethical hacking. · Responsible Hacking: Embrace ethical principles, responsible disclosure, and legal compliance in your journey to become an ethical hacker. · Expert Guidance: Benefit from the expertise of seasoned professionals who have distilled their knowledge into these invaluable books. · Stay Ahead: In the ever-evolving world of cybersecurity, staying updated is crucial. This bundle equips you with the latest insights and strategies. Don't miss this opportunity to become a master of reconnaissance and ethical hacking. Whether you're a beginner or looking to sharpen your skills, the \"RECONNAISSANCE 101\" Book Bundle is your ticket to success in the exciting world of ethical hacking. Secure your copy today and unlock the doors to a promising cybersecurity career!

Advances in Human Factors in Robots, Unmanned Systems and Cybersecurity

This book focuses on the importance of human factors in the development of safe and reliable robotic and unmanned systems. It discusses solutions for improving the perceptual and cognitive abilities of robots, developing suitable synthetic vision systems, coping with degraded reliability in unmanned systems, and predicting robotic behavior in relation to human activities. It covers the design of improved, easy to use, human–system interfaces, together with strategies for increasing human–system performance, and reducing cognitive workload at the user interface. It also discusses real-world applications and case studies of human-robot and human-agent collaboration in different business and educational endeavors. The second part of the book reports on research and developments in the field of human factors in cybersecurity.Contributions cover the technological, social, economic and behavioral aspects of the cyberspace, providing a comprehensive perspective to manage cybersecurity risks. Based on the two AHFE 2021 Conferences such as the AHFE 2021 Conference on Human Factors in Robots, Drones and Unmanned Systems, and the AHFE 2021 Conference on Human Factors in Cybersecurity, held virtually on 25–29 July, 2021, from USA, this book offers extensive information and highlights the importance of multidisciplinary approaches merging engineering, computer science, business and psychological knowledge. It is expected to foster discussion and collaborations between researchers and practitioners with different background, thus stimulating new solutions for the development of reliable and safe, human-centered, highly functional devices to perform automated and concurrent tasks, and to achieve an inclusive, holistic approach for enhancing cybersecurity.

Hacking Essentials

Originally, the term “hacker” referred to a programmer who was skilled in computer operating systems and machine code. Today, it refers to anyone who performs hacking activities. Hacking is the act of changing a system’s features to attain a goal that is not within the original purpose of the creator. The word “hacking” is usually perceived negatively especially by people who do not understand the job of an ethical hacker. In the hacking world, ethical hackers are good guys. What is their role? They use their vast knowledge of computers for good instead of malicious reasons. They look for vulnerabilities in the computer security of organizations and businesses to prevent bad actors from taking advantage of them. For someone that loves the world of technology and computers, it would be wise to consider an ethical hacking career. You get paid (a good amount) to

break into systems. Getting started will not be a walk in the park—just as with any other career. However, if you are determined, you can skyrocket yourself into a lucrative career. When you decide to get started on this journey, you will have to cultivate patience. The first step for many people is usually to get a degree in computer science. You can also get an A+ certification (CompTIA)—you must take and clear two different exams. To be able to take the qualification test, you need to have not less than 500 hours of experience in practical computing. Experience is required, and a CCNA or Network+ qualification to advance your career.

Reconnaissance 101

Introducing the \"RECONNAISSANCE 101\" Book Bundle: Unleash Your Ethical Hacking Potential! Are you ready to embark on a thrilling journey into the world of ethical hacking and information gathering? Look no further, because the \"RECONNAISSANCE 101\" Book Bundle is here to equip you with the essential knowledge and skills you need to excel in this exciting field. ���� BOOK 1: RECONNAISSANCE 101: A BEGINNER'S GUIDE TO FOOTPRINTING & INFORMATION GATHERING If you're new to ethical hacking, this beginner's guide is your perfect starting point. Dive into the fundamentals of reconnaissance and information gathering, learning the ropes of footprinting in a clear and approachable manner. Lay a solid foundation for your ethical hacking journey. ���� BOOK 2: MASTERING FOOTPRINTING: ADVANCED INFORMATION GATHERING STRATEGIES FOR ETHICAL HACKERS Ready to take your skills to the next level? In this volume, you'll explore advanced information gathering techniques used by ethical hackers worldwide. Discover how to navigate the digital landscape with precision and uncover hidden insights to enhance your cybersecurity prowess. ���� BOOK 3: THE ETHICAL HACKER'S FIELD GUIDE TO TARGET DATA ACQUISITION Ethical hacking isn't just about collecting data-it's about doing so responsibly and ethically. Book 3 delves into the principles of responsible data acquisition, ensuring you gather valuable information while maintaining the highest ethical standards. Learn how to identify vulnerabilities and strengthen security. ���� BOOK 4: RECONNAISSANCE PRO: THE ULTIMATE HANDBOOK FOR ELITE INFORMATION GATHERERS Are you ready to become an elite information gatherer? This ultimate handbook will elevate your skills to the highest echelons of the field. Uncover the secrets and tactics employed by the best ethical hackers, propelling you into the realm of elite information gatherers. ���� Why Choose the \"RECONNAISSANCE 101\" Book Bundle? - Comprehensive Knowledge: Covering everything from the basics to elite strategies, this bundle provides a complete understanding of reconnaissance and ethical hacking. - Responsible Hacking: Embrace ethical principles, responsible disclosure, and legal compliance in your journey to become an ethical hacker. - Expert Guidance: Benefit from the expertise of seasoned professionals who have distilled their knowledge into these invaluable books. - Stay Ahead: In the ever-evolving world of cybersecurity, staying updated is crucial. This bundle equips you with the latest insights and strategies. Don't miss this opportunity to become a master of reconnaissance and ethical hacking. Whether you're a beginner or looking to sharpen your skills, the \"RECONNAISSANCE 101\" Book Bundle is your ticket to success in the exciting world of ethical hacking. Secure your copy today and unlock the doors to a promising cybersecurity career!

Hacking Wireless 101

El libro est� dirigido a entusiastas de la inform�tica que desean iniciarse en el interesante tema del hacking �tico de redes inal�mbricas.En �l se describen de forma pr�ctica y amena las t�cnicas usadas por los hackers para explotar vulnerabilidades y penetrar las defensas de las WiFi, de la mano de la popular suite Kali Linux.T�picos cubiertos:* Introducci�n al WiFi Hacking* En qu� consiste el Wardriving* Metodolog�a de un WiFi Hacking* Mapeo inal�mbrico* Ataques a redes y clientes WiFi* C�mo vencer el control por MAC* Ataques a los protocolos WEP, WPA, WPA2* Ataques a WPS* Creaci�n de rogue AP's* Ataques MITM a clientes inal�mbricos y captura de datos* Enga�os a clientes inal�mbricos para burlar el cifrado SSL* Secuestro de sesiones a clientes inal�mbricos* Mecanismos defensivos

Start Hacking Ethically

The Ultimate Beginner's Guide to Ethical Hacking Learn Latest Techniques for Responsible Cyber Defense and Cyber Security This is a Roadmap about Ethical Hacking and how to Fight Against Cybercrime _____ This comprehensive guide offers a unique blend of foundational knowledge, hands-on practice, and cutting-edge trends to transform even the most novice tech enthusiasts into skilled protectors of the digital realm. \"Start Hacking Ethically\" is your ultimate roadmap to becoming a digital defender, equipping you with the tools and expertise to combat cyber threats in an increasingly connected world. Explore the critical principles and guidelines that distinguish ethical hackers from malicious adversaries. Dive into the depths of computer networks, protocols, and cryptography. Master the art of penetration testing and safeguard the most vulnerable corners of the digital landscape, from the cloud to the Internet of Things. Stay ahead of the game with insights into artificial intelligence, machine learning, and the latest trends shaping cybersecurity. Learn how to build a solid incident response plan, and develop essential skills in digital forensics and threat intelligence. Navigate the complex maze of legal and ethical considerations, and discover a rewarding career in ethical hacking. _____ Become an Ethical Hacker by learning about topics like: Identifying and Exploiting Web Vulnerabilities Artificial Intelligence and Machine Learning in Cybersecurity Mobile Device Security and App Testing Virtualization and Containerization for Beginners Understanding Social Engineering Techniques

Learn Ethical Hacking from Scratch

Learn how to hack systems like black hat hackers and secure them like security experts Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to secure systems from hackers Book Description This book starts with the basics of ethical hacking, how to practice hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking,

where you will see how to test the security of wired and wireless networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks. You will also get the hang of post-exploitation techniques, including remotely controlling and interacting with the systems that you compromised. Towards the end of the book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the different fields and types of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how to hack and test the security of systems like professional hackers and security experts.

Learn Python in a Weekend

LEARN PYTHON IN THE FASTEST AND EASIEST WAY Learn Python in a weekend offers you a learning method that will allow you to learn Python in a short period of time, specifically in a weekend!Our experience has demonstrated us that the best way to learn is to do it while having fun and with a methodology that will teach you progressively all the concepts you need to know.In the first part of the book you will find an explanation of the programming language along with an introduction to the programming environment.In the second part of the book you will find a total of 100 exercises of progressive difficulty in which, in addition to guiding you step by step, we explain all the theoretical concepts of programming that you need to know to be able to carry them out. The book contains downloadable material! INDEX 1. Introduction2.- What do I need to start?3.- Learning process4.- Python5.- Development environment6.- Handling of messages on the screen7.- Use of basic data types8.- Control of the flow of a program9.- Loops10.- Project 111.- Functions12.- Project 213.- Basic object-oriented programming14.- Project 315.- Advanced object-oriented programming16.- Working with files17.- Exception control18.- Project 419.- Final Project20.- Annexes

Bulletproof: The Cookbook

In The Bulletproof Diet, Dave Asprey turned conventional diet wisdom on its head, outlining the plan responsible for his 100-pound weight loss, which he came to by \"biohacking\" his body and optimizing every aspect of his health. Asprey urges you to skip breakfast, stop counting calories, eat high levels of healthy saturated fat, work out less, sleep better, and add smart supplements. In doing so, he promises, you'll gain energy, build lean muscle, and watch the pounds melt off--just as he and so many of his devoted followers already have. Bulletproof: The Cookbook picks up where the diet plan leaves off, arming you with 125 recipes to stay bulletproof for life and never get bored. Famous for his butter-laden Bulletproof Coffee, Asprey packs the book with the other delicious, filling meals he uses to maintain his weight loss and sustain his vibrant health.

Computer Hacking

Computer HackingThe Essential Hacking Guide for BeginnersHave you ever wanted to learn more about hacking? Have you wanted to understand the secrets of the hacking community, or understand some of the key techniques used by hackers? Have you wondered about the motivations of hackers, or been intrigued by how people are still targeted by hackers despite the increasing availability of computer security software? If so, then this book is right for you!Hacking is the act of gaining unauthorized access to a computer system, and can include viewing or copying data, or even creating new data. Hacking is more than simply a pastime for those who are interested in technology, and more than simply an illegal activity used for personal gain and with malicious intent, although both of these motivations do make up much of hacking activity. In fact, hacking is its own subculture, and members of the community feel very strongly about their ideologies, techniques and social relationships in the computer underworld. As digital culture continues to grow, it seems that both ethical and unethical hacking will become more and more skilled and its impact evermore significant.This book provides an introduction to the key concepts, techniques and challenges of hacking and includes the following topics: What is hacking Hacking and the influence of cyberpunk The different types of hackers The role of computer security Hacking techniques Tags: hacking, how to hack, hacking exposed, hacking system, hacking 101, hacking for dummies, Hacking Guide, Hacking Essentials, Computer Bugs, Security Breach, internet skills, hacking techniques, Hacking, hacking for dummies, hacking books, hacking guide, how to hack, hacking free guide.

Wireless Hacking 101

WIRELESS HACKING 101 – Piratage éthique des réseaux WiFi sans effort! Ce livre est dédié aux passionnés d'informatique qui cherchent à explorer le monde du piratage éthique et qui veulent se lancer dans les tests d'intrusion sur les réseaux WiFi. Vous y trouverez des informations étape par étape sur la manière d'exploiter les réseaux WiFi à l'aide d'outils inclus dans la populaire distribution Kali Linux, comme la suite aircrack-ng. Sujets traités: Introduction au piratage WiFi En quoi consiste le Wardriving Méthodologie pour un piratage WiFi Analyser les réseaux sans fil Attaquer les réseaux WiFi et ses utilisateurs Contournement du filtrage par MAC Attaques pour les protocoles WEP, WPA, WPA2 Attaques par WPS Création d'un Rogue AP Attaques MITM aux clients WiFi et capture de données Tromper les clients WiFi pour contourner le cryptage SSL Détournement de session des clients WiFi Systèmes de défense

Wireless Hacking 101

Imparate come effettuare test di intrusione wireless facilmente con la suite Kali Linux! WIRELESS HACKING 101 – Come hackerare reti wireless facilmente! Questo libro è diretto agli entusiasti dell'informatica che vogliono specializzarsi nell'interessante settore dell'hacking etico e che vogliono sperimentare con i test di intrusione su reti wireless. Incontrerete informazioni passo a passo su come sfruttare reti Wi-Fi usando alcuni strumenti compresi nella famosa distribuzione Kali Linux, come la suite aircrack-ng. Argomenti trattati: Introduzione al Wi-Fi Hacking In cosa consiste il Wardriving Come procedere ad un Wi-Fi Hacking Monitoraggio di rete Attacchi a reti ed utenti Wi-Fi Come eludere i filtri MAC Attacchi ai protocolli WEP, WPA, WPA2 Attacchi al WPS Creazione di rogue AP Attacchi MITM ad utenti wireless e raccolta dati Come ingannare utenti wireless per eludere la cifratura SSL Dirottare le sessioni di utenti wireless Sistemi difensivi

Ética Hacker

Cuando piensas en hackear, lo que te viene a la mente son códigos complejos y scripts que solo los genios pueden entender. Una vez más, la noción creada por los medios es que las personas maliciosas solo hacen piratería para sus ganancias personales. Sin embargo, hackear no tiene que ser compleja, y no tiene que hacerse por razones maliciosas.La etica hacker, utilizado indistintamente con las pruebas de lápiz, es el tipo de hackers en el que tiene permiso para hackear un sistema para exponer vulnerabilidades y sugerir formas de sellar estas vulnerabilidades para hacer que el sistema de su cliente sea más seguro. Este libro explica todo lo que necesita saber para llevar a cabo un ataque ético, ya sea interna o externamente.En este libro, encontrarás: -Introducción a Hackear: comprenda los términos básicos utilizados en hackear y las diferentes categorías de hacker.-Base de Linux: Dado que Linux es el mejor sistema operativo para hackers, hemos discutido algunas de las características y herramientas básicas que necesitará para ser un hacker ético exitoso. La distribución de Linux BackTrack, desarrollada para hackers, se analiza en profundidad.-Técnicas de Recopilación de Información: Este es el primer paso en la recopilación ética. Aprenderá cómo recopilar información directamente de sus objetivos (recopilación de información activa) e indirectamente (recopilación de información pasiva) y las herramientas que utiliza para hacerlo.-Enumeración de objetivos y escaneo de puertos: Esta es una etapa avanzada en la recopilación de información donde puede encontrar más detalles sobre el host, los puertos abiertos, el sistema operativo y los servicios en ejecución, entre otros detalles.-Evaluar la Vulnerabilidad del Objetivo: Aquí, aprenderá sobre los diferentes escáneres de vulnerabilidad y cómo usarlos para encontrar una puerta de entrada al sistema del objetivo.-Detección de la red del Objetivo: Este capítulo enseña cómo encontrar más detalles sobre la red del objetivo y cómo ubicarse en el centro de la red del objetivo para recopilar más información.-Explotación del lado del Servidor: La etapa de explotación es donde ahora obtiene acceso al sistema del objetivo. En la explotación del lado del servidor, usted explota los hosts y servicios en el sistema del objetivo.-Explotación del Lado del Cliente: Aquí aprenderá cómo comprometer a los usuarios en una red, incluido cómo descifrar contraseñas en función de la información recopilada durante la etapa de recopilación de información.-Explotación posterior / Explotación del objetivo adicional: en este capítulo, aprenderá cómo mantener el acceso en la computadora del objetivo, acceder a más detalles, comprometer más objetivos en la misma red que su primer objetivo y aumentar los privilegios.Solo necesita habilidades informáticas básicas y conocimientos sobre cómo usar el símbolo del sistema para usar este libro. La mayoría de las herramientas se inician y utilizan a través de la línea de comandos en BackTrack. ¡No te dejes intimidar! Es un viaje divertido y lo guiaremos en cada paso.

Internet Business Insights

It's often said that success leaves clues.In Internet Business Insights, Chris Naish and Buck Flogging present interviews from 101 renowned entrepreneurial experts from a diverse range of fields. From those who can teach you to make a comfortable living with internet marketing, to a businesswoman who went from $135k of debt, to selling her company to Bill Gates.

Network Security

Filling the need for a single source that introduces all the important network security areas from a practical perspective, this volume covers technical issues, such as defenses against software attacks by system crackers, as well as administrative topics, such as formulating a security policy. The bestselling author's writing style is highly accessible and takes a vendor-neutral approach.

Seguridad informática - Hacking Ético

Este libro sobre seguridad informática (y hacking etico) está dirigido a todo informático sensibilizado con el concepto de la seguridad informática aunque sea novato o principiante en el dominio de la seguridad de los sistemas de información. Tiene como objetivo iniciar al lector en las técnicas de los atacantes para, así, aprender a defenderse. Esta nueva edición tiene en cuenta las novedades en el campo de la seguridad informática e incluye tres nuevos capítulos que abarcan: la investigación forense, basada principalmente en la investigación de la evidencia digital, ataques más orientados al hardware (como tarjetas con chip y otros) y los routers, omnipresentes en nuestros hogares, poniendo de relieve que no son infalibles y la necesidad de saber configurarlos para evitar problemas. Después de una definición precisa de los diferentes tipos de hackers y de sus objetivos, los autores presentan la metodología de un ataque y los medios para reparar los fallos de seguridad empleados para introducirse en un sistema. El capítulo sobre Ingeniería social, o manipulación social, completamente revisado en esta edición, ilustra que más de un 60% de los ataques con éxito se debe a errores humanos. La captura de huellas digitales, imprescindible antes de lanzar un ataque, se desarrolla ampliamente. Llegamos al corazón de la materia con los fallos físicos, que permiten un acceso directo a ordenadores, y los fallos de red y Wi-Fi se presentan e ilustran cada uno con propuestas de contramedidas.

También se presenta la seguridad en la web y los fallos actuales identificados gracias a la ayuda de herramientas que el lector puede implantar fácilmente en sus propios sistemas. El objetivo es identificar siempre los posibles fallos para establecer después la estrategia de protección adecuada. Siguen, los fallos de sistemasen Windows o Linux con la llegada de nuevas versiones de estos sistemas. Los fallos de aplicación, que introduce algunos elementos para familiarizarse con el lenguaje ensamblador y comprender mejor las posibilidades de ataque. Los tres nuevos capítulos llegan finalmente con el Análisis Forense, los Routers, y los fallos Hardware. El Cloud Computing es abordado (su historia, funcionamiento) para controlar mejor la seguridad. Los autores de este libro forman un equipo de personas con la convicción de que la seguridad informática esté al alcance de todos: \"conocer el ataque para una mejor defensa\" es su lema. Hackers de alma blanca, abren al lector las puertas del conocimiento underground. Los capítulos del libro: Introducción y definiciones – Metodología de un ataque – Elementos de ingeniería social – Toma de huellas – Los fallos físicos – Los fallos de red – Cloud Computing: puntos fuertes y débiles – Los fallos Web – Los fallos de sistema operativo – Los fallos de aplicación – Análisis forense – La seguridad de los routers – Los fallos de hardware

Ethical Hacking

How will governments and courts protect civil liberties in this new era of hacktivism? Ethical Hacking discusses the attendant moral and legal issues. The first part of the 21st century will likely go down in history as the era when ethical hackers opened governments and the line of transparency moved by force. One need only read the motto “we open governments” on the Twitter page for Wikileaks to gain a sense of the sea change that has occurred. Ethical hacking is the non-violent use of a technology in pursuit of a cause—political or otherwise—which is often legally and morally ambiguous. Hacktivists believe in two general but spirited principles: respect for human rights and fundamental freedoms, including freedom of expression and personal privacy; and the responsibility of government to be open, transparent and fully accountable to the public. How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide remains to be seen. What is undisputed is that Ethical Hacking presents a fundamental discussion of key societal questions. A fundamental discussion of key societal questions. This book is published in English. - La première moitié du XXIe siècle sera sans doute reconnue comme l’époque où le piratage éthique a ouvert de force les gouvernements, déplaçant les limites de la transparence. La page twitter de Wikileaks enchâsse cet ethos à même sa devise, « we open governments », et sa volonté d’être omniprésent. En parallèle, les grandes sociétés de technologie comme Apple se font compétition pour produire des produits de plus en plus sécuritaires et à protéger les données de leurs clients, alors même que les gouvernements tentent de limiter et de décrypter ces nouvelles technologies d’encryption. Entre-temps, le marché des vulnérabilités en matière de sécurité augmente à mesure que les experts en sécurité informatique vendent des vulnérabilités de logiciels des grandes technologies, dont Apple et Google, contre des sommes allant de 10 000 à 1,5 million de dollars. L’activisme en sécurité est à la hausse. Le piratage éthique est l’utilisation non-violence d’une technologie quelconque en soutien d’une cause politique ou autre qui est souvent ambigue d’un point de vue juridique et moral. Le hacking éthique peut désigner les actes de vérification de pénétration professionnelle ou d’experts en sécurité informatique, de même que d’autres formes d’actions émergentes, comme l’hacktivisme et la désobéissance civile en ligne. L’hacktivisme est une forme de piratage éthique, mais également une forme de militantisme des droits civils à l’ère numérique. En principe, les adeptes du hacktivisme croient en deux grands principes : le respect des droits de la personne et les libertés fondamentales, y compris la liberté d’expression et à la vie privée, et la responsabilité des gouvernements d’être ouverts, transparents et pleinement redevables au public. En pratique, toutefois, les antécédents comme les agendas des hacktivistes sont fort diversifiés. Il n’est pas clair de quelle façon les tribunaux et les gouvernements traiteront des tentatives de piratage eu égard aux zones grises juridiques, aux approches éthiques conflictuelles, et compte tenu du fait qu’il n’existe actuellement, dans le monde, presque aucune exception aux provisions, en matière de cybercrime et de crime informatique, liées à la recherche sur la sécurité ou l’intérêt public. Il sera également difficile de déterminer le lien entre hacktivisme et droits civils. Ce livre est publié en anglais.

The Hacker Ethic

The Hacker Ethic takes us on a journey through fundamental questions about life in the information age - a trip of constant surprises, after which our time and our lives can be seen from unexpected perspectives.Nearly a century ago, Max Weber's The Protestant Ethic and the Spirit of Capitalism articulated the animating spirit of the industrial age, the Protestant ethic. In the original meaning of the word, hackers are enthusiastic computer programmers who share their work with others; they are not computer criminals. Now Pekka Himanen - together with Linus Torvalds and Manuel Castells - articulates how hackers represent a new opposing ethos for the information age.Underlying hackers' technical creations - such as the Internet and the personal computer, which have become symbols of our time - are the hacker values that produced them. These values promote passionate and freely rhythmed work; the belief that individuals can create great things by joining forces in imaginative ways; and the need to maintain our existing ethical ideals, such as privacy and equality, in our new increasingly technologized society.

Study Hacks

This book, which is filled with study hacks and study tips to work less while getting straight-a's, will solve your student life problems! Have we ever been taught of how to study? No... There's no need to study for long periods of time when you can study in half of the time but more effectively, by only using specific study tips for college, high-school or school in general! There's no need to lose your mind when it comes to study for a test. There are simple study tips, used by highly-successful students, that will help you to get good grades in college! In this guide you'll learn how to: Make sure you're physically and mentally prepared to study successfully Create a revision timetable that you'll actually be able to stick to Avoid information overload and focus your studies on the things you need to know to ace your exams Produce top quality revision notes that you'll use again and again Prepare for your exams without letting revision take over your life The way you study is full of unscientific

methods which makes the entire process feel like drudgery. What if someone taught you how to study just once the right way without any distractions and still remember and recollect everything? The second block teaches you the hacks to study effectively with minimal efforts. The way you write exams makes the entire difference. You being a knowledge treasure house is useless if you don't master the art of reproducing it in the exam.

The Moral Status of Technical Artefacts

This book considers the question: to what extent does it make sense to qualify technical artefacts as moral entities? The authors’ contributions trace recent proposals and topics including instrumental and non-instrumental values of artefacts, agency and artefactual agency, values in and around technologies, and the moral significance of technology. The editors’ introduction explains that as ‘agents’ rather than simply passive instruments, technical artefacts may actively influence their users, changing the way they perceive the world, the way they act in the world and the way they interact with each other. This volume features the work of various experts from around the world, representing a variety of positions on the topic. Contributions explore the contested discourse on agency in humans and artefacts, defend the Value Neutrality Thesis by arguing that technological artefacts do not contain, have or exhibit values, or argue that moral agency involves both human and non-human elements. The book also investigates technological fields that are subject to negative moral valuations due to the harmful effects of some of their products. It includes an analysis of some difficulties arising in Artificial Intelligence and an exploration of values in Chemistry and in Engineering. The Moral Status of Technical Artefacts is an advanced exploration of the various dimensions of the relations between technology and morality

Weapons of Math Destruction

A former Wall Street quant sounds an alarm on the mathematical models that pervade modern life - and threaten to rip apart our social fabric We live in the age of the algorithm. Increasingly, the decisions that affect our lives - where we go to school, whether we get a loan, how much we pay for insurance - are being made not by humans, but by mathematical models. In theory, this should lead to greater fairness: everyone is judged according to the same rules, and bias is eliminated. And yet, as Cathy O'Neil reveals in this urgent and necessary book, the opposite is true. The models being used today are opaque, unregulated, and incontestable, even when they're wrong. Most troubling, they reinforce discrimination. Tracing the arc of a person's life, O'Neil exposes the black box models that shape our future, both as individuals and as a society. These \"weapons of math destruction\" score teachers and students, sort CVs, grant or deny loans, evaluate workers, target voters, and monitor our health. O'Neil calls on modellers to take more responsibility for their algorithms and on policy makers to regulate their use. But in the end, it's up to us to become more savvy about the models that govern our lives. This important book empowers us to ask the tough questions, uncover the truth, and demand change.

Hacking the Hacker

Meet the world's top ethical hackers and explore the tools of the trade Hacking the Hacker takes you inside the world of cybersecurity to show you what goes on behind the scenes, and introduces you to the men and women on the front lines of this technological arms race. Twenty-six of the world's top white hat hackers, security researchers, writers, and leaders, describe what they do and why, with each profile preceded by a no-experience-necessary explanation of the relevant technology. Dorothy Denning discusses advanced persistent threats, Martin Hellman describes how he helped invent public key encryption, Bill Cheswick talks about firewalls, Dr. Charlie Miller talks about hacking cars, and other cybersecurity experts from around the world detail the threats, their defenses, and the tools and techniques they use to thwart the most advanced criminals history has ever seen. Light on jargon and heavy on intrigue, this book is designed to be an introduction to the field; final chapters include a guide for parents of young hackers, as well as the Code of Ethical Hacking to help you start your own journey to the top. Cybersecurity is becoming increasingly critical at all levels, from retail businesses all the way up to national security. This book drives to the heart of the field, introducing the people and practices that help keep our world secure. Go deep into the world of white hat hacking to grasp just how critical cybersecurity is Read the stories of some of the world's most renowned computer security experts Learn how hackers do what they do—no technical expertise necessary Delve into social engineering, cryptography, penetration testing, network attacks, and more As a field, cybersecurity is large and multi-faceted—yet not historically diverse. With a massive demand for qualified professional that is only going to grow, opportunities are endless. Hacking the Hacker shows you why you should give the field a closer look.

Hacking ético con herramientas Python

En los últimos años, Python se ha convertido en un lenguaje muy adoptado por la industria de la seguridad informática, debido a su simpleza, practicidad, además de ser un lenguaje tanto interpretado como de scripting. Su integración con multitud de librerías de terceros hace pensar en Python como un lenguaje con múltiples posibilidades tanto desde el punto de vista ofensivo como defensivo de la seguridad y ha sido utilizado para un gran número de proyectos incluyendo programación Web, herramientas de seguridad, scripting y automatización de tareas. El objetivo del libro es capacitar a aquellos interesados en la seguridad, a aprender a utilizar Python como lenguaje de programación, no solo para poder construir aplicaciones, sino también para automatizar y especificar muchas de las tareas que se realizan durante un proceso de auditoría de seguridad. Repasaremos desde los conceptos básicos de programación hasta construir nuestra propia herramienta de análisis y extracción de información. Con el objetivo de extraer información de servidores y servicios que están ejecutando, información como nombres de dominio y banners, conoceremos los módulos que ofrece python para extraer información que los servidores exponen de forma pública y veremos los módulos que permiten extraer metadatos de documentos e imágenes, así como

extraer información de geolocalización a partir de direcciones IP y nombres de dominio. También analizaremos conceptos más avanzados, como implementar nuestro propio escáner de puertos con comandos nmap y scapy, además de cómo conectarnos desde python con servidores FTP, SSH, SNMP, Metaspoit y escáneres de vulnerabilidades como nexpose.

101 Ethical Dilemmas

Will meat eaters get into heaven? Do trees have rights? Is it ever right to design a baby? What would you do? Would you always do the right thing? Is there a right thing? In this second edition of his thought-provoking and highly engaging introduction to ethics, Martin Cohen brings us eleven brand new ethical dilemmas including: The Dodgy Donor Clinic The Famous Footbridge Dilemma The Human Canonball. From overcrowded lifeboats to the censor's pen, Martin Cohen's stimulating and amusing dilemmas reveal the subtleties, complexities and contradictions that make up the rich tapestry of ethics. From DIY babies and breeding experiments to 'Twinkies courtroom drama' and Newgate Prison, there is a dilemma for everyone. This book may not help you become a good person, but at least you will have had a good think about it.

Subliminal Psychology 101

People can be so resistant to your ideas. Wouldn't you like to be able to slip into someone's mind and make him or her do your bidding? Since the days of crazy CIA mind control experiments, a series of highly secretive methods of subliminal mind control have been available. But they have been kept under wraps because of their power. Now you can find them out for yourself and make your life what you want it to be by gaining control over the minds of others. Subliminal psychology is a special and top secret science that explores how to enter someone's subconscious mind. There, you can plant ideas that the person will start acting on without knowing why. Using signals, gestures, images, scents, sounds, touch, and words, you can influence someone tremendously and very stealthily. No one will know why they do the things they do under your influence. Subliminal psychology has a huge variety of uses. In this book, you will learn how to use it for seduction and settling conflict in your personal relationships. You will also use it to beat the odds in competitions. You will learn how to use it to make work better for you, and to gain dominance over others. You will learn how to apply it to parenting and relationships of all kinds. Finally, you will learn how to utilize it on yourself to bring out your best, end bad habits, and build confidence and self-esteem through positive thinking. Hack your own mind. Or hack others'. The secrets to how are all in these pages.

Terrorism and the media

This text introduces the spirit and theory of hacking as well as the science behind it all; it also provides some core techniques and tricks of hacking so you can think like a hacker, write your own hacks or thwart potential system attacks.

Hacking- The art Of Exploitation

This open access book provides the first comprehensive collection of papers that provide an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies.

The Ethics of Cybersecurity

THIS IS THE SYSTEM OPERATOR. WHO IS USING THIS ACCOUNT? PLEASE IDENTIFY YOURSELF... Vicky's life is completely normal. Maybe even a little boring. But all that changes when her dad is accused of stealing a million pounds from the bank where he works. Vicky knows for sure that her dad is innocent, and is determined to prove it. Luckily for him, she is a seasoned computer hacker. Using the skills he taught her, she's going to attempt to break the bank's files. Should be simple, right? But it's a race against time to find the cyber-thief, before they find her . . . 'A page-turner' - Sunday Express 'Accept the expertise and race along with the plot' - Observer

Hacker

Cutting-edge techniques for finding and fixing critical security flaws Fortify your network and avert digital catastrophe with proven strategies from a team of security experts. Completely updated and featuring 13 new chapters, Gray Hat Hacking, The Ethical Hacker’s Handbook, Fifth Edition explains the enemy’s current weapons, skills, and tactics and offers field-tested remedies, case studies, and ready-to-try testing labs. Find out how hackers gain access, overtake network devices, script and inject malicious code, and plunder Web applications and browsers. Android-based exploits, reverse engineering techniques, and cyber law are thoroughly covered in this state-of-the-art resource. And the new topic of exploiting the Internet of things is introduced in this edition. •Build and launch spoofing exploits with Ettercap •Induce error conditions and crash software using fuzzers •Use advanced reverse engineering to exploit Windows and Linux software •Bypass Windows Access Control and memory protection schemes •Exploit web applications with Padding Oracle Attacks •Learn the use-after-free technique used in

recent zero days •Hijack web browsers with advanced XSS attacks •Understand ransomware and how it takes control of your desktop •Dissect Android malware with JEB and DAD decompilers •Find one-day vulnerabilities with binary diffing •Exploit wireless systems with Software Defined Radios (SDR) •Exploit Internet of things devices •Dissect and exploit embedded devices •Understand bug bounty programs •Deploy next-generation honeypots •Dissect ATM malware and analyze common ATM attacks •Learn the business side of ethical hacking

Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition

You don’t need to be a wizard to transform a game you like into a game you love. Imagine if you could give your favorite PC game a more informative heads-up display or instantly collect all that loot from your latest epic battle. Bring your knowledge of Windows-based development and memory management, and Game Hacking will teach you what you need to become a true game hacker. Learn the basics, like reverse engineering, assembly code analysis, programmatic memory manipulation, and code injection, and hone your new skills with hands-on example code and practice binaries. Level up as you learn how to: –Scan and modify memory with Cheat Engine –Explore program structure and execution flow with OllyDbg –Log processes and pinpoint useful data files with Process Monitor –Manipulate control flow through NOPing, hooking, and more –Locate and dissect common game memory structures You’ll even discover the secrets behind common game bots, including: –Extrasensory perception hacks, such as wallhacks and heads-up displays –Responsive hacks, such as autohealers and combo bots –Bots with artificial intelligence, such as cave walkers and automatic looters Game hacking might seem like black magic, but it doesn’t have to be. Once you understand how bots are made, you’ll be better positioned to defend against them in your own games. Journey through the inner workings of PC games with Game Hacking, and leave with a deeper understanding of both game design and computer security.

Game Hacking

Hackers exploit browser vulnerabilities to attack deep withinnetworks The Browser Hacker's Handbook gives a practicalunderstanding of hacking the everyday web browser and using it as abeachhead to launch further attacks deep into corporate networks.Written by a team of highly experienced computer security experts,the handbook provides hands-on tutorials exploring a range ofcurrent attack methods. The web browser has become the most popular and widely usedcomputer \"program\" in the world. As the gateway to the Internet, itis part of the storefront to any business that operates online, butit is also one of the most vulnerable entry points of any system.With attacks on the rise, companies are increasingly employingbrowser-hardening techniques to protect the unique vulnerabilitiesinherent in all currently used browsers. The Browser Hacker'sHandbook thoroughly covers complex security issues and exploresrelevant topics such as: Bypassing the Same Origin Policy ARP spoofing, social engineering, and phishing to accessbrowsers DNS tunneling, attacking web applications, andproxying—all from the browser Exploiting the browser and its ecosystem (plugins andextensions) Cross-origin attacks, including Inter-protocol Communicationand Exploitation The Browser Hacker's Handbook is written with aprofessional security engagement in mind. Leveraging browsers aspivot points into a target's network should form an integralcomponent into any social engineering or red-team securityassessment. This handbook provides a complete methodology tounderstand and structure your next browser penetration test.

The Browser Hacker's Handbook

\"A fantastic book for anyone looking to learn the tools and techniques needed to break in and stay in.\" --Bruce Potter, Founder, The Shmoo Group \"Very highly recommended whether you are a seasoned professional or just starting out in the security business.\" --Simple Nomad, Hacker

Gray Hat Hacking, Second Edition

Explains how to take advantage of Google's user interface, discussing how to filter results, use Google's special services, integrate Google applications into a Web site or Weblog, write information retrieval programs, and play games.

Google Hacks

This book explains strategies, techniques, legal issues and the relationships between digital resistance activities, information warfare actions, liberation technology and human rights. It studies the concept of authority in the digital era and focuses in particular on the actions of so-called digital dissidents. Moving from the difference between hacking and computer crimes, the book explains concepts of hacktivism, the information war between states, a new form of politics (such as open data movements, radical transparency, crowd sourcing and “Twitter Revolutions”), and the hacking of political systems and of state technologies. The book focuses on the protection of human rights in countries with oppressive regimes.

Resistance, Liberation Technology and Human Rights in the Digital Age

https://uk.fulldoc.me/doc/160926/440117M8Q8/planning-the_life__you__desire-living-the-life-you-deserve_creating__achieving__goals-that_matter-most_your_all-in_one_personal-strategic-plan__new_years-resolutions_life__guidebook.pdf
https://uk.fulldoc.me/play/L32B158/160926/size_48_15mb_cstephenmurray_vector_basics-answer__key__2009.pdf
https://uk.fulldoc.me/doc/223941/8H7J764/honda__ntv600__revere__ntv650__and-ntv650v_deauville_service-and_repair-manual-hardcover.pdf
https://uk.fulldoc.me/edu/223941/3R201V8/sound-engineering_tutorials-free.pdf
https://uk.fulldoc.me/pdf/28MT711395/52MT874/apache_nifi-51-interview__questions_hdf-hortonworks__dataflow.pdf
https://uk.fulldoc.me/ppt/160926/7D6C676624/hidden__star-stars-of_mithra.pdf
https://uk.fulldoc.me/pdf/va/4434222A8V260916/comparative-constitutionalism__cases_and__materials_american__casebook_series.pdf
https://uk.fulldoc.me/text/eo/46E141O/from__genes_to__genomes_concepts__and_applications_of-dna_technology.pdf
https://uk.fulldoc.me/chap/bw/768B1W6617260916/new__science-in-everyday_life_class_7-answers.pdf