# TOR DARKNET BUNDLE 5 In 1 Master The ART OF INVISIBILITY Bitcoins Hacking Kali Linux

As recognized, adventure as capably as experience nearly lesson, amusement, as competently as covenant can be gotten by just checking out a books **TOR DARKNET BUNDLE 5 In 1 Master The ART OF INVISIBILITY Bitcoins Hacking Kali Linux** furthermore it is not directly done, you could give a positive response even more roughly this life, on the world.

We meet the expense of you this proper as capably as easy exaggeration to get those all. We have the funds for TOR DARKNET BUNDLE 5 In 1 Master The ART OF INVISIBILITY Bitcoins Hacking Kali Linux and numerous book collections from fictions to scientific research in any way. accompanied by them is this TOR DARKNET BUNDLE 5 In 1 Master The ART OF INVISIBILITY Bitcoins Hacking Kali Linux that can be your partner.

*Hacking* - Jeff Simon 2016-09-18
This Book, Hacking Practical Guide for Beginners is a comprehensive learning material for all inexperienced hackers. It is a short manual that describes the essentials of hacking. By reading this book, you'll arm yourself with modern hacking knowledge and techniques. However, do take note that this material is not limited to theoretical information. It also contains a myriad of practical tips, tricks, and strategies that you can use in hacking your targets. The first chapter of this book explains the basics of hacking and the different types of hackers. The second chapter has a detailed study plan for budding hackers. That study plan will help you improve your skills in a short period of time. The third chapter will teach you how to write your own codes using the Python programming language. The rest of the book contains detailed instructions on how you can become a skilled hacker and penetration tester. After reading this book, you'll learn how to: - Use the Kali Linux operating system - Set up a rigged WiFi hotspot - Write codes and programs using Python - Utilize the Metasploit framework in attacking your targets - Collect information using certain hacking tools - Conduct a penetration test - Protect your computer and network from other hackers - And a lot more... Make sure you get your copy today!
*Digital Painting Techniques* - 3dtotal.Com, 2012-10-12
Discover the tips, tricks and techniques that really work for concept artists, matte painters and animators. Compiled by the team at 3dtotal.com, Digital Painting Techniques, Volume 1 offers digital inspiration with hands-on insight and techniques from professional digital artists. More than just a gallery book - within Digital Painting Techniques each artist has written a breakdown overview, with supporting imagery of how they made their piece of work. Beginner and intermediate digital artists will be inspired by the gallery style collection of the finest examples of digital painting from world renowned digital artists. Start your mentorship into the world of digital painting today with some of the greatest digital artists in the world and delve into professional digital painting techiques, such as speed painting, custom brush creation and matte painting. Develop your digital painting skills beyond the variety of free online digital painting tutorials and apply the most up to date techniques to your digital canvas with Digital Painting Techniques for Animators.
Linux Basics for Hackers - OccupyTheWeb 2018-12-04
This practical, tutorial-style book uses the Kali Linux distribution to teach Linux basics with a focus on how hackers would use them. Topics include Linux command line basics, filesystems, networking, BASH basics, package management, logging, and the Linux kernel and drivers. If you're getting started along the exciting path of hacking, cybersecurity, and pentesting, Linux Basics for Hackers is an excellent first step. Using Kali Linux, an advanced penetration testing distribution of Linux, you'll learn the basics of using the Linux operating system and acquire the tools and techniques you'll need to take control of a Linux environment. First, you'll learn how to install Kali on a virtual machine and get an introduction to basic Linux concepts. Next, you'll tackle broader Linux topics like manipulating text, controlling file and directory permissions, and managing user environment variables. You'll then focus in on foundational hacking concepts like security and anonymity and learn scripting skills with bash and Python. Practical tutorials and exercises throughout will reinforce and test your skills as you learn how to: - Cover your tracks by changing your network information and manipulating the rsyslog logging utility - Write a tool to scan for network connections, and connect and listen to wireless networks - Keep your internet activity stealthy using Tor, proxy servers, VPNs, and encrypted email - Write a bash script to scan open ports for potential targets - Use and abuse services like MySQL, Apache web server, and OpenSSH - Build your own hacking tools, such as a remote video spy camera and a password cracker Hacking is complex, and there is no single way in. Why not start at the beginning with Linux Basics for Hackers?
**TOR DARKNET BUNDLE (5 in 1) Master the ART OF INVISIBILITY** - Lance Henderson 2022-08-22
The #1 Killer Anonymity Package - 5 Books for the Price of 1! Darknet: The ULTIMATE Guide on the Art of Invisibility Want to surf the web anonymously? Cloak yourself in shadow? I will show you how to become a ghost in the machine - leaving no tracks back to your ISP. This book covers it all! Encrypting your files, securing your PC, masking your online footsteps with Tor browser, VPNs, Freenet and Bitcoins, and all while giving you peace of mind with TOTAL 100% ANONYMITY. - How to Be Anonymous Online AND Offline - Step by Step Guides for Tor, Freenet, I2P, VPNs, Usenet and more - Browser Fingerprinting - Anti-Hacking and Counter-forensics Techniques - Photo & Video Metadata - How to Encrypt Files (I make this super simple) - How to Defeat NSA Spying - How to Browse the Deep Web - How to Protect Your Identity - How to Hide Anything! Tor & The Dark Art of Anonymity The NSA hates Tor. So does the FBI. Even Google wants it gone, as do Facebook and Yahoo and every other soul-draining, identity-tracking vampiric media cartel that scans your emails and spies on your private browsing sessions to better target you - but there's hope. This manual will give you the incognito tools that will make you a master of anonymity! Covered in Tor: - Browse the Internet Anonymously - Darkcoins, Darknet Marketplaces & Opsec Requirements - Tor Hidden Servers - How to Not Get Caught - Counter-Forensics the FBI Doesn't Want You to Know About! - Windows vs. Linux Network Security - Cryptocurrency (Real Bitcoin Anonymity) - Supercookies & Encryption - Preventing Marketers and Debt Collectors From Finding You - How to Protect Your Assets - Home, Money & Family! - How to Hide Anything from even the most trained IRS agents The Invisibility Toolkit Within this book lies top secrets

known only to the FBI and a few law enforcement agencies: How to disappear in style and retain assets. How to switch up multiple identities on the fly and be invisible such that no one; not your ex, not your parole officer, nor even the federal government can find you. Ever. You'll learn: - How to disappear overseas - How to wear a perfect disguise. - How to bring down a drone. - How to be invisible in Canada, Thailand, China or the Philippines. - How to use Bitcoin on the run. - How to fool skip tracers, child support courts, student loan collectors - How to sneak into Canada - How to be anonymous online using Tor, Tails and the Internet Underground - Edward Snowden's biggest mistake. Usenet: The Ultimate Guide The first rule of Usenet: Don't Talk About Usenet! But times have changed and you want what you want. Usenet is the way to go. I will show you: - How to use Usenet - which groups to join, which to avoid - How to be anonymous online - Why Usenet is better than torrents - How to use Tor, How to use PGP, Remailers/Mixmaster, SSL. - How to encrypt your files - Which Vpn and Usenet companies rat you out, and which won't. - How to Stay Anonymous Online You've probably read The Hacker Playbook by Peter Kim and the Art of Invisibility by Kevin Mitnick. While they are fine books, you need this super pack to take it to the NEXT LEVEL. Scroll to the top of the page and select the "buy" button and wear a cloak of invisibility TODAY!

Hacklog Volume 1 Anonymity (English Version): It Security & Ethical Hacking Handbook - Stefano Novelli 2019-03-22

Have you ever wished to become a hacker? If the answer is yes, this book is for you!Started as a crowdfunding project, Hacklog Volume 1: Anonymity is the first of a book collection dedicated to who wants to enter the world of Hacking and IT Security. You'll learn how to use the tools real-life hackers leverage everyday to avoid controls, how to conceal your most hidden files (and also how to recover them!) and you'll get a deeper insight over the broad world of anonymity.Hacklog Volume 1: Anonymity was designed for who is not too familiar with IT Security, but is willing to learn! Furthermore, it's a good review opportunity for those who already know this fascinating world as well as industry experts: High Schools, Universities, Industry Professionals and other Bodies use Hacklog to get information and stay up-to-date about the techniques used by cyber criminals to avoid controls and stay completely anonymous in the broad world of the Web.Here are some of the themes covered by the first volume: * You'll learn how to use the Operating Systems used by hackers and industry experts, including Ubuntu, Kali Linux, Parrot Security OS and many others, based both on GNU/Linux and Windows and macOS.* You'll be able to identify the traces left on a computer during an attack or an IT inspection, like MAC Address, Hostnames usage, DNSs and the via-Proxy anonymizing IP* You'll be able to make secure communications through the VPNs, discovering the best service providers and the regulations about governmental takedowns* You'll learn the vast world of the Deep Web and the Dark Net, the TOR, I2P and Freenet anonymizing circuits, as well as the Combo Networks to stay safe through pyramidal communication tunnels* You'll be able to identify the local resources that can harm you, like Cookies, JavaScript, Flash, Java, ActiveX, WebRTC and you will learn how to fingerprint your browser* You'll learn how to protect your data, verifying it with checksums and encrypting it using techniques like PGP and GPG; furthermore, you will get information about how to encrypt a disk, steganography and how to backup your crucial data* You'll be able to recover data even after a disk wipe, and destroy it irreversibly, using the same techniques used by the law enforcement bodies around the world* You'll learn how to identify the vulnerabilities that expose your identity to the Web, and the best practice to prevent it* You'll learn how to anonymously purchase from the Web, using the Dark Net circuits and crypto-currencies like the BitcoinHacklog, Volume 1: Anonymity is an open project, partially released under Italian Creative Commons 4.0 - Italy. You can find all licensing information at our official website: www.hacklog.ne

Weaving the Dark Web - Robert W. Gehl 2018-08-14

An exploration of the Dark Web—websites accessible only with special routing software—that examines the history of three anonymizing networks, Freenet, Tor, and I2P. The term “Dark Web” conjures up drug markets, unregulated gun sales, stolen credit cards. But, as Robert Gehl points out in Weaving the Dark Web, for each of these illegitimate uses, there are other, legitimate ones: the New York Times's anonymous whistleblowing system, for example, and the use of encryption by political dissidents. Defining the Dark Web straightforwardly as websites that can be accessed only with special routing software, and noting the frequent use of “legitimate” and its variations by users, journalists, and law enforcement to describe Dark Web practices (judging them “legit” or “sh!t”), Gehl uses the concept of legitimacy as a window into the Dark Web. He does so by examining the history of three Dark Web systems: Freenet, Tor, and I2P. Gehl presents three distinct meanings of legitimate: legitimate force, or the state's claim to a monopoly on violence; organizational propriety; and authenticity. He explores how Freenet, Tor, and I2P grappled with these different meanings, and then discusses each form of legitimacy in detail by examining Dark Web markets, search engines, and social networking sites. Finally, taking a broader view of the Dark Web, Gehl argues for the value of anonymous political speech in a time of ubiquitous surveillance. If we shut down the Dark Web, he argues, we lose a valuable channel for dissent.

Mac OS X and iOS Internals - Jonathan Levin 2012-11-05

An in-depth look into Mac OS X and iOS kernels Powering Macs, iPhones, iPads and more, OS X and iOS are becoming ubiquitous. When it comes to documentation, however, much of them are shrouded in mystery. Cocoa and Carbon, the application frameworks, are neatly described, but system programmers find the rest lacking. This indispensable guide illuminates the darkest corners of those systems, starting with an architectural overview, then drilling all the way to the core. Provides you with a top down view of OS X and iOS Walks you through the phases of system startup—both Mac (EFi) and mobile (iBoot) Explains how processes, threads, virtual memory, and filesystems are maintained Covers the security architecture Reviews the internal Apis used by the system—BSD and Mach Dissects the kernel, XNU, into its sub components: Mach, the BSD Layer, and I/o kit, and explains each in detail Explains the inner workings of device drivers From architecture to implementation, this book is essential reading if you want to get serious about the internal workings of Mac OS X and iOS.

**Mastering CentOS 7 Linux Server** - Mohamed Alibi 2016-01-29

Configure, manage, and secure a CentOS 7 Linux server to serve a variety of services provided in a sustainable computer's infrastructure. About This Book Learn how to efficiently set up and manage a Linux server using one of the best suited technologies for this purpose, CentOS 7 Personalize your Linux server and familiarize yourself with the latest tools and utilities setup provided by the new CentOS distribution Follow a step-by-step tutorial through the configuration of the requested services with the capacity to personalize them as per your needs Who This Book Is For If you are a Linux system administrator with an intermediate administration level, this is your opportunity to master the brand new distribution of CentOS. If you wish to possess a fully sustainable Linux server, with all its new tools and tweaks, that serves a variety of services to your users

and customers, this book is ideal for you. It is your ticket to easily adapt to all the changes made in the latest shift. What You Will Learn Manage CentOS 7 users, groups, and root access privileges Enhance the server's security through its firewall and prevent the most common attacks from penetrating or disabling the server Explore and implement the common, useful services that a CentOS 7 server can provide Monitor your server infrastructure for system or hardware issues Create and configure a virtual machine using virtualization technologies Implement a cloud computing solution on a single node system Get an introduction to the configuration management tools and their usage Discover the importance of the tools that provide remote connection, server service security, and system and process monitoring tools In Detail Most server infrastructures are equipped with at least one Linux server that provides many essential services, both for a user's demands and for the infrastructure itself. Setting up a sustainable Linux server is one of the most demanding tasks for a system administrator to perform. However, learning multiple, new technologies to meet all of their needs is time-consuming. CentOS 7 is the brand new version of the CentOS Linux system under the RPM (Red Hat) family. It is one of the most widely-used operating systems, being the choice of many organizations across the world. With the help of this book, you will explore the best practices and administration tools of CentOS 7 Linux server along with implementing some of the most common Linux services. We start by explaining the initial steps you need to carry out after installing CentOS 7 by briefly explaining the concepts related to users, groups, and right management, along with some basic system security measures. Next, you will be introduced to the most commonly used services and shown in detail how to implement and deploy them so they can be used by internal or external users. Soon enough, you will be shown how to monitor the server. We will then move on to master the virtualization and cloud computing techniques. Finally, the book wraps up by explaining configuration management and some security tweaks. All these topics and more are covered in this comprehensive guide, which briefly demonstrates the latest changes to all of the services and tools with the recent shift from CentOS 6 to CentOS 7. Style and approach This is a detailed and in-depth guide to help you administrate CentOS 7 for the usage of your server's infrastructure and also for personal network security. Each section shows a list of tools and utilities that are useful to perform the required task, in an easy to understand manner.

**Ethical Hacking and Cybersecurity** - Itc Academy 2021-01-28

Does the word "hacking" scare you? Do you know if your personal information was stolen from your account? Have you always wanted to learn how to protect your system from such attacks? Do you want to learn the secrets of ethical hackers? If you answered yes to all these questions, you've come to the right place. Generally, hacking has earned a negative reputation and has become associated with cyberattacks and breaches in cybersecurity. But this is not always true. If this is your first book on hacking, you will become more acquainted with the world of hacking as this book gives a simple overview of ethical hacking. The term "ethical hacker" emerged in the late 1970s when the US government hired expert groups called "red teams" to hack their own computer system. Hackers are cyber-experts who lawfully or illegally hack. You enter the security system of a computer network to retrieve or recollect information. This book will talk about: WHAT IS ETHICAL HACKING WHO SHOULD I PROTECT MY BUSINESS FROM? SKILLS EVERY HACKER NEEDS DIFFERENT TYPES OF HACKING OVER THE YEARS HACKING RISKS FOR BUSINESSES PROTECTING BUSINESSES FROM CYBERCRIME PROTECTING YOUR FAMILY FROM CYBER ATTACKS SECRET SOCIAL MEDIA HACKS YOU WANT TO TRY NOW ..AND MUCH, MUCH MORE! This book bundle is perfect for beginners, a comprehensive guide that will show you the easy way to overcoming cybersecurity, computer hacking, wireless network and penetration testing. So if you want to learn more about Cybersecurity and Ethical Hacking, scroll up and click "add to cart"!

**Beginning Ethical Hacking with Kali Linux** - Sanjib Sinha 2018-11-29

Get started in white-hat ethical hacking using Kali Linux. This book starts off by giving you an overview of security trends, where you will learn the OSI security architecture. This will form the foundation for the rest of Beginning Ethical Hacking with Kali Linux. With the theory out of the way, you'll move on to an introduction to VirtualBox, networking, and common Linux commands, followed by the step-by-step procedure to build your own web server and acquire the skill to be anonymous . When you have finished the examples in the first part of your book, you will have all you need to carry out safe and ethical hacking experiments. After an introduction to Kali Linux, you will carry out your first penetration tests with Python and code raw binary packets for use in those tests. You will learn how to find secret directories on a target system, use a TCP client in Python, and scan ports using NMAP. Along the way you will discover effective ways to collect important information, track email, and use important tools such as DMITRY and Maltego, as well as take a look at the five phases of penetration testing. The coverage of vulnerability analysis includes sniffing and spoofing, why ARP poisoning is a threat, how SniffJoke prevents poisoning, how to analyze protocols with Wireshark, and using sniffing packets with Scapy. The next part of the book shows you detecting SQL injection vulnerabilities, using sqlmap, and applying brute force or password attacks. Besides learning these tools, you will see how to use OpenVas, Nikto, Vega, and Burp Suite. The book will explain the information assurance model and the hacking framework Metasploit, taking you through important commands, exploit and payload basics. Moving on to hashes and passwords you will learn password testing and hacking techniques with John the Ripper and Rainbow. You will then dive into classic and modern encryption techniques where you will learn the conventional cryptosystem. In the final chapter you will acquire the skill of exploiting remote Windows and Linux systems and you will learn how to own a target completely. What You Will LearnMaster common Linux commands and networking techniques Build your own Kali web server and learn to be anonymous Carry out penetration testing using Python Detect sniffing attacks and SQL injection vulnerabilities Learn tools such as SniffJoke, Wireshark, Scapy, sqlmap, OpenVas, Nikto, and Burp Suite Use Metasploit with Kali Linux Exploit remote Windows and Linux systemsWho This Book Is For Developers new to ethical hacking with a basic understanding of Linux programming.

*Mastering Kali Linux Wireless Pentesting* - Jilumudi Raghu Ram 2016-02-25

Test your wireless network's security and master advanced wireless penetration techniques using Kali Linux About This Book Develop your skills using attacks such as wireless cracking, Man-in-the-Middle, and Denial of Service (DOS), as well as extracting sensitive information from wireless networks Perform advanced wireless assessment and penetration tests Use Embedded Platforms, Raspberry PI, and Android in wireless penetration testing with Kali Linux Who This Book Is For If you are an intermediate-level wireless security consultant in Kali Linux and want to be the go-to person for Kali Linux wireless security in your organisation, then this is the book for you. Basic understanding of the core Kali Linux concepts is expected. What You Will Learn Fingerprint wireless networks with the various

tools available in Kali Linux Learn various techniques to exploit wireless access points using CSRF Crack WPA/WPA2/WPS and crack wireless encryption using Rainbow tables more quickly Perform man-in-the-middle attack on wireless clients Understand client-side attacks, browser exploits, Java vulnerabilities, and social engineering Develop advanced sniffing and PCAP analysis skills to extract sensitive information such as DOC, XLS, and PDF documents from wireless networks Use Raspberry PI and OpenWrt to perform advanced wireless attacks Perform a DOS test using various techniques and tools In Detail Kali Linux is a Debian-based Linux distribution designed for digital forensics and penetration testing. It gives access to a large collection of security-related tools for professional security testing - some of the major ones being Nmap, Aircrack-ng, Wireshark, and Metasploit. This book will take you on a journey where you will learn to master advanced tools and techniques to conduct wireless penetration testing with Kali Linux. You will begin by gaining an understanding of setting up and optimizing your penetration testing environment for wireless assessments. Then, the book will take you through a typical assessment from reconnaissance, information gathering, and scanning the network through exploitation and data extraction from your target. You will get to know various ways to compromise the wireless network using browser exploits, vulnerabilities in firmware, web-based attacks, client-side exploits, and many other hacking methods. You will also discover how to crack wireless networks with speed, perform man-in-the-middle and DOS attacks, and use Raspberry Pi and Android to expand your assessment methodology. By the end of this book, you will have mastered using Kali Linux for wireless security assessments and become a more effective penetration tester and consultant. Style and approach This book uses a step-by-step approach using real-world attack scenarios to help you master the wireless penetration testing techniques.

**Programming with MicroPython** - Nicholas H. Tollervey 2017-09-25

It’s an exciting time to get involved with MicroPython, the re-implementation of Python 3 for microcontrollers and embedded systems. This practical guide delivers the knowledge you need to roll up your sleeves and create exceptional embedded projects with this lean and efficient programming language. If you’re familiar with Python as a programmer, educator, or maker, you’re ready to learn—and have fun along the way. Author Nicholas Tollervey takes you on a journey from first steps to advanced projects. You’ll explore the types of devices that run MicroPython, and examine how the language uses and interacts with hardware to process input, connect to the outside world, communicate wirelessly, make sounds and music, and drive robotics projects. Work with MicroPython on four typical devices: PyBoard, the micro:bit, Adafruit’s Circuit Playground Express, and ESP8266/ESP32 boards Explore a framework that helps you generate, evaluate, and evolve embedded projects that solve real problems Dive into practical MicroPython examples: visual feedback, input and sensing, GPIO, networking, sound and music, and robotics Learn how idiomatic MicroPython helps you express a lot with the minimum of resources Take the next step by getting involved with the Python community

**Ingredient Branding** - Philip Kotler 2010-05-17

An Ingredient Brand is exactly what the name implies: an ingredient or component of a product that has its own brand identity. This is the first comprehensive book that explains how Ingredient Branding works and how brand managers can successfully improve the performance of component marketing. The authors have examined more than one hundred examples, analyzed four industries and developed nine detailed case studies to demonstrate the viability of this marketing innovation. The new concepts and principles can easily be applied by professionals. In the light of the success stories of Intel, GoreTex, Dolby, TetraPak, Shimano, and Teflon it can be expected that component suppliers will increasingly use Ingredient Branding strategies in the future.

*Tor* - Evan Lane 2017-03-31

Set Up TOR in 2017! Tor, also known as the Dark Net, is an interesting look at an alternative way to surf the internet. This book will discuss what Tor is, a step by step guide on how to download and access it as well as some of the different types of things the user can do while browsing the internet. You will find information on the use of pseudonyms (an important and intriguing part of using Tor), anonymity, bitcoins, and additional layers of security you can add to ensure any information you seek on the internet will be completely concealed from prying eyes. This book will also provide you the reader with basic information on the differences between cookies and supercookies as well as ways to keep their computer safe from both. You will also get insight into how Tor came to be, some of the campaigns against Tor orchestrated by the NSA and other government agencies and how those were thwarted by the designers of this alternate online universe. Discover everything about TOR now by clicking the Buy Button on this page!

**Tor and the Dark Art of Anonymity** - Lance Henderson 2022-08-22

Tired of being spied on? Sometimes a victim decides to stop being a victim. Master the dark art of anonymity today and get instant access to thousands of deep web hidden websites, portals and secret files plus access to the Hidden Wiki, all for free. The evidence is in: It's 1984 and the surveillance powers that be possess a special hatred for individual thought, free speech and online privacy. That means most 3 letter agencies as well as most Big Brother groups like Google, Facebook and Twitter. You're being tracked left, right and center. Today's written word will be used against you in the future. Don't let a tyrannical future bite you in your backside. It's time to FIGHT BACK. Other books tell you to install this or that and leave it at that. This book goes much deeper, delving into the very heart of invisibility, offline and on: how to create a new darknet persona and leave no electronic trail...with Tor or a hundred other apps. In essence, how to be anonymous without looking like you're trying to be anonymous. Covered: - Darknet Marketplaces & Opsec - Why Silk Road Failed - Cryptocurrency - The Hidden Wiki - What To Do If Caught - How to Run a Hidden Server on the Deep Web - Linux Encryption & Mobile Tor - Darknet Personas - Police Raids - How to Survive a Police Interrogation - How Hacking Groups like Anonymous and Reloaded stay hidden. - Opsec for dealing in exotic contraband - Cybersecurity secrets And much more! Don't wait. If you love privacy, freedom and the democratic way of life, this is your chance to learn in hours, not years, what most alphabet agencies like the FBI and NSA already know. Do not wait until a farenheit 451 situation erupts and reading these kinds of books will be forbidden. The greatest risk to evil thriving is when good men do nothing. Buy today and take anonymity to the next level. Because tomorrow may be too late!

Dark Web - Hsinchun Chen 2011-12-16

The University of Arizona Artificial Intelligence Lab (AI Lab) Dark Web project is a long-term scientific research program that aims to study and understand the international terrorism (Jihadist) phenomena via a computational, data-centric approach. We aim to collect "ALL" web content generated by international terrorist groups, including web sites, forums, chat rooms, blogs, social networking sites, videos, virtual world, etc. We have developed various multilingual data mining, text mining, and web mining techniques to perform link analysis, content analysis, web metrics (technical sophistication) analysis, sentiment analysis, authorship analysis, and video analysis in our research. The

approaches and methods developed in this project contribute to advancing the field of Intelligence and Security Informatics (ISI). Such advances will help related stakeholders to perform terrorism research and facilitate international security and peace. This monograph aims to provide an overview of the Dark Web landscape, suggest a systematic, computational approach to understanding the problems, and illustrate with selected techniques, methods, and case studies developed by the University of Arizona AI Lab Dark Web team members. This work aims to provide an interdisciplinary and understandable monograph about Dark Web research along three dimensions: methodological issues in Dark Web research; database and computational techniques to support information collection and data mining; and legal, social, privacy, and data confidentiality challenges and approaches. It will bring useful knowledge to scientists, security professionals, counterterrorism experts, and policy makers. The monograph can also serve as a reference material or textbook in graduate level courses related to information security, information policy, information assurance, information systems, terrorism, and public policy.

**When Gadgets Betray Us** - Robert Vamosi 2011-03-29
Looks at the important issues that are often overlooked in the race to find the best, fastest, and most cutting-edge technological wonders.

Digital Art Masters: - 3dtotal.Com, 2012-11-12
Meet some of the finest 2D and 3D artists working in the industry today and discover how they create some of the most innovative digital art in the world. More than a gallery book or a coffee table book- Digital Art Masters Volume 5 includes over 50 artists and 900 unique and stunning 2D and 3D digital art. Beyond the breath taking images is a breakdown of the techniques, challenges and tricks the artists employed while creating stunning imagery. This volume, much like the previous volumes is not your standard coffee table book nor is it our usual how-to-book. New to this volume will be 5 artist video tutorials. Five artists will specifically detail an aspect of their gallery image from start to finish, offering further technique driven insight and expertise offering 2 1□2 hours of additional inspiration. With a click of a mouse, artists willbe able to apply the leading techniques to their own work with access to additional video tutorials, source files, textures and digital brushes at the companion website: http://www.focalpress.com/digital-art-masters/index.html .

*Tor and the Dark Net* - James Smith 2016-03-21
So many people take their privacy on the internet for granted. Some may know and choose to ignore the fact, but every single thing you do online is being tracked and guess what? For better or for worse it is there forever. Whether you're simply browsing websites or you are accessing confidential information that you would rather no one know about, there are ways to remain anonymous.

**Cybercrime** - David Wall 2007-09-17
Looking at the full range of cybercrime, and computer security he shows how the increase in personal computing power available within a globalized communications network has affected the nature of and response to criminal activities. We have now entered the world of low impact, multiple victim crimes in which bank robbers, for example, no longer have to meticulously plan the theft of millions of dollars. New technological capabilities at their disposal now mean that one person can effectively commit millions of robberies of one dollar each. Against this background, David Wall scrutinizes the regulatory challenges that cybercrime poses for the criminal (and civil) justice processes, at both the national and the international levels. Book jacket.

**Hacking for Beginners** - Julian James McKinnon 2021-03-29
-- 55% OFF for Bookstores! -- Hacking is a term most of us shudder away from; we assume that it is only for those who have lots of programming skills and loose morals and that it is too hard for us to learn how to use it. But what if you could work with hacking like a good thing, as a way to protect your own personal information and even the information of many customers for a large business? This guidebook is going to spend some time taking a look at the world of hacking and some of the great techniques that come with this type of process as well. Whether you are an unethical or ethical hacker, you will use a lot of the same techniques, and this guidebook is going to explore them in more detail along the way, turning you from a novice to a professional in no time. Some of the different topics we will look at concerning hacking in this guidebook includes: The basics of hacking and some of the benefits of learning how to use this programming technique. The different types of hackers, why each one is important, and how they are different from one another. How to work with your own penetration test. The importance of strong passwords and how a professional hacker will attempt to break through these passwords. A look at how to hack through a website of any company that doesn't add in the right kind of security to the mix. A look at how to hack through the different wireless networks that are out there to start a man-in-the-middle attack or another attack. Some of the other common attacks that we need to work with including man-in-the-middle, denial-of-service attack malware, phishing, and so much more. Some of the steps that you can take in order to ensure that your network will stay safe and secure, despite all of the threats out there. Hacking is a term that most of us do not know that much about. We assume that only a select few can use hacking to gain their own personal advantage and that it is too immoral or too hard for most of us to learn. But learning a bit about hacking can actually be the best way to keep your own network safe. Are you ready to learn more about hacking and what it can do to the safety and security of your personal or business network?

**Cybersecurity For Dummies** - Joseph Steinberg 2019-10-01
Protect your business and family against cyber attacks Cybersecurity is the protection against the unauthorized or criminal use of electronic data and the practice of ensuring the integrity, confidentiality, and availability of information. Being "cyber-secure" means that a person or organization has both protected itself against attacks by cyber criminals and other online scoundrels, and ensured that it has the ability to recover if it is attacked. If keeping your business or your family safe from cybersecurity threats is on your to-do list, Cybersecurity For Dummies will introduce you to the basics of becoming cyber-secure! You'll learn what threats exist, and how to identify, protect against, detect, and respond to these threats, as well as how to recover if you have been breached! The who and why of cybersecurity threats Basic cybersecurity concepts What to do to be cyber-secure Cybersecurity careers What to think about to stay cybersecure in the future Now is the time to identify vulnerabilities that may make you a victim of cyber-crime – and to defend yourself before it is too late.

**The Art of Invisibility** - Kevin Mitnick 2019-09-10
Real-world advice on how to be invisible online from "the FBI's most-wanted hacker" (Wired) Your every step online is being tracked and stored, and your identity easily stolen. Big companies and big governments want to know and exploit what you do, and privacy is a luxury few can afford or understand. In this explosive yet practical book, computer-security expert Kevin Mitnick uses true-life stories to show exactly what is happening without your knowledge, and teaches you "the art of invisibility": online and everyday tactics to protect

you and your family, using easy step-by-step instructions. Reading this book, you will learn everything from password protection and smart Wi-Fi usage to advanced techniques designed to maximize your anonymity. Invisibility isn't just for superheroes--privacy is a power you deserve and need in the age of Big Brother and Big Data.

**Hacking with Kali Linux: a Guide to Ethical Hacking** - Grzegorz Nowak 2019-10-22

▶ Are you interested in learning more about hacking and how you can use these techniques to keep yourself and your network as safe as possible? ▶ Would you like to work with Kali Linux to protect your network and to make sure that hackers are not able to get onto your computer and cause trouble or steal your personal information? ▶ Have you ever been interested in learning more about the process of hacking, how to avoid being taken advantage of, and how you can use some of techniques for your own needs? This guidebook is going to provide us with all of the information that we need to know about Hacking with Linux. Many people worry that hacking is a bad process and that it is not the right option for them. The good news here is that hacking can work well for not only taking information and harming others but also for helping you keep your own network and personal information as safe as possible. Inside this guidebook, we are going to take some time to explore the world of hacking, and why the Kali Linux system is one of the best to help you get this done. We explore the different types of hacking, and why it is beneficial to learn some of the techniques that are needed to perform your own hacks and to see the results that we want with our own networks. In this guidebook, we will take a look at a lot of the different topics and techniques that we need to know when it comes to working with hacking on the Linux system. Some of the topics that we are going to take a look at here include: The different types of hackers that we may encounter and how they are similar and different. How to install the Kali Linux onto your operating system to get started. The basics of cybersecurity, web security, and cyberattacks and how these can affect your computer system and how a hacker will try to use you. The different types of malware that hackers can use against you. How a man in the middle, DoS, Trojans, viruses, and phishing can all be tools of the hacker. And so much more. Hacking is often an option that most people will not consider because they worry that it is going to be evil, or that it is only used to harm others. But as we will discuss in this guidebook, there is so much more to the process than this. ★ When you are ready to learn more about hacking with Kali Linux and how this can benefit your own network and computer, make sure to check out this guidebook to get started!

*The Pentester BluePrint* - Phillip L. Wylie 2020-10-27

JUMPSTART YOUR NEW AND EXCITING CAREER AS A PENETRATION TESTER The Pentester BluePrint: Your Guide to Being a Pentester offers readers a chance to delve deeply into the world of the ethical, or "white-hat" hacker. Accomplished pentester and author Phillip L. Wylie and cybersecurity researcher Kim Crawley walk you through the basic and advanced topics necessary to understand how to make a career out of finding vulnerabilities in systems, networks, and applications. You'll learn about the role of a penetration tester, what a pentest involves, and the prerequisite knowledge you'll need to start the educational journey of becoming a pentester. Discover how to develop a plan by assessing your current skillset and finding a starting place to begin growing your knowledge and skills. Finally, find out how to become employed as a pentester by using social media, networking strategies, and community involvement. Perfect for IT workers and entry-level information security professionals, The Pentester BluePrint also belongs on the bookshelves of anyone seeking to transition to the exciting and in-demand field of penetration testing. Written in a highly approachable and accessible style, The Pentester BluePrint avoids unnecessarily technical lingo in favor of concrete advice and practical strategies to help you get your start in pentesting. This book will teach you: The foundations of pentesting, including basic IT skills like operating systems, networking, and security systems The development of hacking skills and a hacker mindset Where to find educational options, including college and university classes, security training providers, volunteer work, and self-study Which certifications and degrees are most useful for gaining employment as a pentester How to get experience in the pentesting field, including labs, CTFs, and bug bounties

*Hacking]* - Julian James McKinnon 2021-03-08

-- 55% OFF for Bookstores -- Hacking: three books in one Would you like to learn more about the world of hacking and Linux? Yes? Then you are in the right place.... Included in this book collection are: Hacking for Beginners: A Step by Step Guide to Learn How to Hack Websites, Smartphones, Wireless Networks, Work with Social Engineering, Complete a Penetration Test, and Keep Your Computer Safe Linux for Beginners: A Step-by-Step Guide to Learn Architecture, Installation, Configuration, Basic Functions, Command Line and All the Essentials of Linux, Including Manipulating and Editing Files Hacking with Kali Linux: A Step by Step Guide with Tips and Tricks to Help You Become an Expert Hacker, to Create Your Key Logger, to Create a Man in the Middle Attack and Map Out Your Own Attacks Hacking is a term most of us shudder away from. We assume that it is only for those who have lots of programming skills and loose morals and that it is too hard for us to learn how to use it. But what if you could work with hacking like a good thing, as a way to protect your own personal information and even the information of many customers for a large business? This guidebook is going to spend some time taking a look at the world of hacking, and some of the great techniques that come with this type of process as well. Whether you are an unethical or ethical hacker, you will use a lot of the same techniques, and this guidebook is going to explore them in more detail along the way, turning you from a novice to a professional in no time. Are you ready to learn more about hacking and what you are able to do with this tool?

Web Penetration Testing with Kali Linux - Juned Ahmed Ansari 2015-11-26

Build your defense against web attacks with Kali Linux 2.0 About This Book Gain a deep understanding of the flaws in web applications and exploit them in a practical manner Get hands-on web application hacking experience with a range of tools in Kali Linux 2.0 Develop the practical skills required to master multiple tools in the Kali Linux 2.0 toolkit Who This Book Is For If you are already working as a network penetration tester and want to expand your knowledge of web application hacking, then this book tailored for you. Those who are interested in learning more about the Kali Sana tools that are used to test web applications will find this book a thoroughly useful and interesting guide. What You Will Learn Set up your lab with Kali Linux 2.0 Identify the difference between hacking a web application and network hacking Understand the different techniques used to identify the flavor of web applications Expose vulnerabilities present in web servers and their applications using server-side attacks Use SQL and cross-site scripting (XSS) attacks Check for XSS flaws using the burp suite proxy Find out about the mitigation techniques used to negate the effects of the Injection and Blind SQL attacks In Detail Kali Linux 2.0 is the new generation of the industry-leading BackTrack Linux penetration testing and security auditing Linux distribution. It contains several hundred tools aimed at

various information security tasks such as penetration testing, forensics, and reverse engineering. At the beginning of the book, you will be introduced to the concepts of hacking and penetration testing and will get to know about the tools used in Kali Linux 2.0 that relate to web application hacking. Then, you will gain a deep understanding of SQL and command injection flaws and ways to exploit the flaws. Moving on, you will get to know more about scripting and input validation flaws, AJAX, and the security issues related to AJAX. At the end of the book, you will use an automated technique called fuzzing to be able to identify flaws in a web application. Finally, you will understand the web application vulnerabilities and the ways in which they can be exploited using the tools in Kali Linux 2.0. Style and approach This step-by-step guide covers each topic with detailed practical examples. Every concept is explained with the help of illustrations using the tools available in Kali Linux 2.0.

**Hacking** - Erickson Karnel 2021-01-04

4 Manuscripts in 1 Book!Have you always been interested and fascinated by the world of hacking Do you wish to learn more about networking?Do you want to know how to protect your system from being compromised and learn about advanced security protocols?If you want to understand how to hack from basic level to advanced, keep reading... This book set includes: Book 1) Hacking for Beginners: Step by Step Guide to Cracking codes discipline, penetration testing and computer virus. Learning basic security tools on how to ethical hack and grow Book 2) Hacker Basic Security: Learning effective methods of security and how to manage the cyber risks. Awareness program with attack and defense strategy tools. Art of exploitation in hacking. Book 3) Networking Hacking: Complete guide tools for computer wireless network technology, connections and communications system. Practical penetration of a network via services and hardware. Book 4) Kali Linux for Hackers: Computer hacking guide. Learning the secrets of wireless penetration testing, security tools and techniques for hacking with Kali Linux. Network attacks and exploitation. The first book "Hacking for Beginners" will teach you the basics of hacking as well as the different types of hacking and how hackers think. By reading it, you will not only discover why they are attacking your computers, but you will also be able to understand how they can scan your system and gain access to your computer. The second book "Hacker Basic Security" contains various simple and straightforward strategies to protect your devices both at work and at home and to improve your understanding of security online and fundamental concepts of cybersecurity. The third book "Networking Hacking" will teach you the basics of a computer network, countermeasures that you can use to prevent a social engineering and physical attack and how to assess the physical vulnerabilities within your organization. The fourth book "Kali Linux for Hackers" will help you understand the better use of Kali Linux and it will teach you how you can protect yourself from most common hacking attacks. Kali-Linux is popular among security experts, it allows you to examine your own systems for vulnerabilities and to simulate attacks. Below we explain the most exciting parts of the book set. An introduction to hacking. Google hacking and Web hacking Fingerprinting Different types of attackers Defects in software The basics of a computer network How to select the suitable security assessment tools Social engineering. How to crack passwords. Network security Linux tools Exploitation of security holes The fundamentals and importance of cybersecurity Types of cybersecurity with threats and attacks How to prevent data security breaches Computer virus and prevention techniques Cryptography And there's so much more to learn! Follow me, and let's dive into the world of hacking!Don't keep waiting to start your new journey as a hacker; get started now and order your copy today!

Computer Programming Bible - C. P. A Inc 2020-01-23

Whether your incentive to learn about computer programming stems from interest, or it's because you want a better paying job, starting with the basics and working your way up is the most promising approach to take.

*The Darkest Web (Dyslexic Edition)* - Eileen Ormsby 2018

Hitmen for hire, drugs for sale. Inside the dangerous world that lurks beneath the bright, friendly light of your internet screen. Eileen Ormsby has spent the past five years exploring every corner of the Dark Web. She has shopped on darknet markets, contributed to forums, waited in red rooms and been threatened by hitmen on murder-for-hire sites. On occasions, her dark web activities have poured out into the real world and she has attended trials, met with criminals and the law enforcement who tracked them down, interviewed dark web identities and visited them in prison. This book will take you into the murkiest depths of the web's dark underbelly: a place of hitmen for hire, red rooms, hurtcore sites and markets that will sell anything a person is willing to pay for - including another person. The Darkest Web.

**The Dark Web Dive** - John Forsay 2019-06-15

Notorious. Illegal. Avoid if you can. These are words most commonly used to describe what some mistakenly call 'The Deep Web'. Yet, the Deep Web is where your banking information sits. Your shopping profile, your saved searches, and your passwords. What they're really referring to is THE DARK WEB, and I'll take you there--with the proper preparation and knowledge of its history. Learn who created the Dark Web and how long it's been in existence. Discover the people who dedicated their lives to the technology that runs the Dark Web, and why they made such sacrifices. You'll read about those who rose to dizzying heights plumbing riches in the darknet, and who fell because of their vanity and overconfidence. In The Dark Web Dive, you'll unbury the facts about: The secret origin of Tor and the Tor Project The uncensored history of the Dark Web, Arpanet and its dark siblings Who provides funding for the Dark Web? (You'll be surprised.) The stories behind the Silk Road, Hansa, and other infamous Dark Web marketplaces. The truth about the Surface Web and why Google is not to be trusted with your information, and what you can do about it? The technology you need to keep your internet identity safe on a daily basis. The chilling tales of the Dark Web. Are the urban legends coming from the darknets based in truth? Who are the heroes, and who are the villains of hidden service sites? And how to tell one from another? A step-by-step guide to suit up before you embark on your own Dark Web Dive. The answers you've always wanted to the questions you were perhaps too afraid to ask are here, along with a wealth of knowledge to open your eyes as to what's really happening below the surface of the Internet every day. Be one of the ones who know the truth and has the facts to arm themselves against identity theft and data farming. Dare to take The Dark Web Dive today!

**Cult of the Dead Cow** - Joseph Menn 2019-06-04

The shocking untold story of the elite secret society of hackers fighting to protect our privacy, our freedom -- even democracy itself Cult of the Dead Cow is the tale of the oldest, most respected, and most famous American hacking group of all time. Though until now it has remained mostly anonymous, its members invented the concept of hacktivism, released the top tool for testing password security, and created what was for years the best technique for controlling computers from afar, forcing giant companies to work harder to protect customers. They contributed to the development of Tor, the most important privacy tool on the net, and helped build cyberweapons that advanced US security without injuring anyone. With its origins in the earliest days

of the Internet, the cDc is full of oddball characters -- activists, artists, even future politicians. Many of these hackers have become top executives and advisors walking the corridors of power in Washington and Silicon Valley. The most famous is former Texas Congressman and current presidential candidate Beto O'Rourke, whose time in the cDc set him up to found a tech business, launch an alternative publication in El Paso, and make long-shot bets on unconventional campaigns. Today, the group and its followers are battling electoral misinformation, making personal data safer, and battling to keep technology a force for good instead of for surveillance and oppression. Cult of the Dead Cow shows how governments, corporations, and criminals came to hold immense power over individuals and how we can fight back against them.

Tribe of Hackers - Marcus J. Carey 2019-07-23

Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781119643371) was previously published as Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781793464187). While this version features a new cover design and introduction, the remaining content is the same as the prior release and should not be considered a new or updated product. Looking for real-world advice from leading cybersecurity experts? You've found your tribe. Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World is your guide to joining the ranks of hundreds of thousands of cybersecurity professionals around the world. Whether you're just joining the industry, climbing the corporate ladder, or considering consulting, Tribe of Hackers offers the practical know-how, industry perspectives, and technical insight you need to succeed in the rapidly growing information security market. This unique guide includes inspiring interviews from 70 security experts, including Lesley Carhart, Ming Chow, Bruce Potter, Robert M. Lee, and Jayson E. Street. Get the scoop on the biggest cybersecurity myths and misconceptions about security Learn what qualities and credentials you need to advance in the cybersecurity field Uncover which life hacks are worth your while Understand how social media and the Internet of Things has changed cybersecurity Discover what it takes to make the move from the corporate world to your own cybersecurity venture Find your favorite hackers online and continue the conversation Tribe of Hackers is a must-have resource for security professionals who are looking to advance their careers, gain a fresh perspective, and get serious about cybersecurity with thought-provoking insights from the world's most noteworthy hackers and influential security specialists.

*Hacking with Kali Linux: Penetration Testing* - Grzegorz Nowak 2019-10-27

▶ Hacking is something that is taking over the world. ▶ With more and more people are moving online and doing almost any task that they can there, it is likely that hacking and other similar attacks are just going to increase over time. ▶ Our personal, financial, and business information is all found online, and this is a big goldmine for hackers all throughout the world. It is so important that we learn the best way to take care of our personal and financial information and to make sure that we are protected against any hacking attack that comes our way. And working with Kali Linux to do a penetration test can be one of the best ways that we learn where the vulnerabilities of our system lie, and how to protect against a hacker using them against us. This guidebook is going to spend some time looking at how to complete a penetration test with the Kali Linux system, and how we can use this to keep our own networks safe. In addition to working with the penetration test, we will also explore how to work with protecting our identity online, how to download the Kali Linux system in a variety of manners, and how to work with other hacking techniques so we can always be on the lookout against those who are trying to attack us maliciously. In this guidebook, we are going to explore penetration testing, along with a wide variety of other topics that work with hacking on Kali Linux. Some of the topics that we will explore in this guidebook include: How to set up the Kali Linux operating system to work on your computer and the different methods that you can do. How to work with the boot drive version of Kali Linux. Some of the commands that you can send over to your terminal to get the best results. Some of the basics of the Kali Linux network that we need to know before our penetration test. The dark web and the Tor program, and how these can help a hacker stay anonymous. The importance of the VPN, or virtual private networks, and how those can keep the hacker hidden from view. Some of the simple hacking techniques that a hacker could use against a network or a system. The basics and the methodologies of penetration testing. The stages that we need to follow to make penetration testing happen. There is so much that we can do to protect our own computers and networks and to make sure that no one is able to come onto the system and cause a mess by stealing our personal information. ★ When you are ready to learn how to work on Penetration Testing with Kali Linux, make sure to check out this guidebook to help you get started!

Linux Hardening in Hostile Networks - Kyle Rankin 2017-07-17

Implement Industrial-Strength Security on Any Linux Server In an age of mass surveillance, when advanced cyberwarfare weapons rapidly migrate into every hacker's toolkit, you can't rely on outdated security methods—especially if you're responsible for Internet-facing services. In Linux® Hardening in Hostile Networks, Kyle Rankin helps you to implement modern safeguards that provide maximum impact with minimum effort and to strip away old techniques that are no longer worth your time. Rankin provides clear, concise guidance on modern workstation, server, and network hardening, and explains how to harden specific services, such as web servers, email, DNS, and databases. Along the way, he demystifies technologies once viewed as too complex or mysterious but now essential to mainstream Linux security. He also includes a full chapter on effective incident response that both DevOps and SecOps can use to write their own incident response plan. Each chapter begins with techniques any sysadmin can use quickly to protect against entry-level hackers and presents intermediate and advanced techniques to safeguard against sophisticated and knowledgeable attackers, perhaps even state actors. Throughout, you learn what each technique does, how it works, what it does and doesn't protect against, and whether it would be useful in your environment. Apply core security techniques including 2FA and strong passwords Protect admin workstations via lock screens, disk encryption, BIOS passwords, and other methods Use the security-focused Tails distribution as a quick path to a hardened workstation Compartmentalize workstation tasks into VMs with varying levels of trust Harden servers with SSH, use apparmor and sudo to limit the damage attackers can do, and set up remote syslog servers to track their actions Establish secure VPNs with OpenVPN, and leverage SSH to tunnel traffic when VPNs can't be used Configure a software load balancer to terminate SSL/TLS connections and initiate new ones downstream Set up standalone Tor services and hidden Tor services and relays Secure Apache and Nginx web servers, and take full advantage of HTTPS Perform advanced web server hardening with HTTPS forward secrecy and ModSecurity web application firewalls Strengthen email security with SMTP relay authentication, SMTPS, SPF records, DKIM, and DMARC Harden DNS servers, deter their use in DDoS attacks, and fully implement DNSSEC Systematically protect databases via network access control, TLS

traffic encryption, and encrypted data storage Respond to a compromised server, collect evidence, and prevent future attacks Register your product at informit.com/register for convenient access to downloads, updates, and corrections as they become available.

Hacker Basic Security - Karnel Erickson 2020-10-29

Do you wish to learn some tools of basic security? Do you want to find out how to protect yourself and your data from online attacks? Hacking has never been more important than now! Keep reading if you want to learn more... In our daily life we are constantly connected, using our computer or phones in order to access and share information online. While these various connections help improve our online life, they also pose a cause for concern on what they are sharing and that's why it's important to understand what cybersecurity mean. Knowledge is power! The book "Hacker Basic Security" contains various simple and straightforward strategies to protect your devices both at work and at home and to improve your understanding of security online and fundamental concepts of cybersecurity. The book extensively explores various topics including - The fundamentals and importance of cybersecurity - The various types of cybersecurity with threats and attacks - Cybersecurity basics: Protect your computer network against virus and malware - Breaches in cybersecurity - The types and ways of preventing data security breaches - Malware - Attacks, types, and analysis - Computer virus and prevention techniques - Basic concepts of cryptography - The assumptions of hackers/attackers - The benefits, drawbacks, and future of cryptography - An extensive topic on virtual private networks And there's so much more to learn! "Hacker Basic Security" provides an insight into everything concerning cybersecurity even if you have no technical knowledge about it. Hacking is real, and what better way to protect yourself than being pro-active and arming yourself with the knowledge on how it works and what you can do against it. Get yourself furnish with the significance of having a cybersecurity plan with practical guidance to deal and manage threats such as insider threat, data breaches, malware, virus, ransomware, denial-of-service, and worms. You can change the narrative with this book and that begins with you downloading this book and opening yourself up to a whole new world of possibilities! Scroll to the top and select the "BUY" button to start enjoying this amazing deal instantly.

**Spindrift** - Anna Burke 2020-08-25

Can a hot summer fling mend the hearts of two broken women? Morgan Donovan had everything she ever wanted: a dream job as a large animal veterinarian, awesome friends, and a loving and supportive fiancée. But it all comes crashing down when her fiancée dumps her after realizing that Morgan’s job will always come first. And, while Morgan still has the job and friends, her heart is broken into a million tiny pieces. Emilia Russo is a burned-out shelter vet. When the unexpected death of her father triggers a mental breakdown that hastens the end of her relationship, she retreats to his house in Seal Cove, Maine. She plans on spending the summer renovating it while she figures out how to pull the pieces of her life back together. But when she runs into Morgan at the dock where her father’s sailboat is moored, her plans for a quiet summer of healing and reflection sink like a stone—the attraction is immediate and obvious, and Emilia finds herself slipping seamlessly into Morgan’s world Each woman knows this fling will end when Emilia returns to Boston at the end of the summer, but they’re unprepared for the intensity and depth of their attraction. And, as the gales of fall begin to drive leaves like spindrift upon Seal Cove, Morgan and Emilia must each come to terms with how much they’re willing to give up to stay together.

*JFK Has Been Shot* - Charles A. Crenshaw 2013-10-01

The “thrilling, dramatic, historic” #1 New York Times bestseller by the Parkland Hospital surgeon who fought to save President John F. Kennedy (Robert K. Tanenbaum). On November 22, 1963, Dr. Charles Crenshaw, an accomplished surgeon, tried to save John F. Kennedy’s life—and then days later, the life of the alleged assassin, Lee Harvey Oswald. His gripping, firsthand account contradicts the Warren Commission and years of public misperception to illuminate a chapter in American history long cloaked in conspiracy. Writing with eye-opening immediacy, Dr. Crenshaw takes readers into the emergency room to share the critical events at Parkland Hospital as he lived them. Now updated, his searing testimony punctures myths and shatters a cover-up of massive proportions. “Hard-hitting, courageous, and correct in every respect.”—Cyril Wecht, M.D., J.D. "Dr. Crenshaw offers his expert opinion with persuasive evidence. Read this page-turning account of the Kennedy assassination.”—Robert K. Tanenbaum, Deputy Chief Counsel, Congressional Committee Investigation into the Assassination of President Kennedy Includes revealing photos Previously published as JFK Conspiracy of Silence

How to Find Out Anything - Don MacLeod 2012-08-07

In How to Find Out Anything, master researcher Don MacLeod explains how to find what you're looking for quickly, efficiently, and accurately—and how to avoid the most common mistakes of the Google Age. Not your average research book, How to Find Out Anything shows you how to unveil nearly anything about anyone. From top CEO’s salaries to police records, you’ll learn little-known tricks for discovering the exact information you’re looking for. You’ll learn: •How to really tap the power of Google, and why Google is the best place to start a search, but never the best place to finish it. •The scoop on vast, yet little-known online resources that search engines cannot scour, such as refdesk.com, ipl.org, the University of Michigan Documents Center, and Project Gutenberg, among many others. •How to access free government resources (and put your tax dollars to good use). •How to find experts and other people with special knowledge. •How to dig up seemingly confidential information on people and businesses, from public and private companies to non-profits and international companies. Whether researching for a term paper or digging up dirt on an ex, the advice in this book arms you with the sleuthing skills to tackle any mystery.

**Hands-On Penetration Testing on Windows** - Phil Bramwell 2018-07-30

Master the art of identifying vulnerabilities within the Windows OS and develop the desired solutions for it using Kali Linux. Key Features Identify the vulnerabilities in your system using Kali Linux 2018.02 Discover the art of exploiting Windows kernel drivers Get to know several bypassing techniques to gain control of your Windows environment Book Description Windows has always been the go-to platform for users around the globe to perform administration and ad hoc tasks, in settings that range from small offices to global enterprises, and this massive footprint makes securing Windows a unique challenge. This book will enable you to distinguish yourself to your clients. In this book, you'll learn advanced techniques to attack Windows environments from the indispensable toolkit that is Kali Linux. We'll work through core network hacking concepts and advanced Windows exploitation techniques, such as stack and heap overflows, precision heap spraying, and kernel exploitation, using coding principles that allow you to leverage powerful Python scripts and shellcode. We'll wrap up with post-exploitation strategies that enable you to go deeper and keep your access. Finally, we'll introduce kernel hacking fundamentals and fuzzing testing, so you can discover vulnerabilities and write custom exploits. By the end of this book, you'll be well-versed in identifying vulnerabilities within the Windows OS and developing the desired solutions for

them. What you will learn Get to know advanced pen testing techniques with Kali Linux Gain an understanding of Kali Linux tools and methods from behind the scenes See how to use Kali Linux at an advanced level Understand the exploitation of Windows kernel drivers Understand advanced Windows concepts and protections, and how to bypass them using Kali Linux Discover Windows exploitation techniques, such as stack and heap overflows and kernel exploitation, through coding principles Who this book is for This book is for penetration testers, ethical hackers, and individuals breaking into the pentesting role after demonstrating an advanced skill in boot camps. Prior experience with Windows exploitation, Kali Linux, and some Windows debugging tools is necessary