Tor Darknet Bundle 5 In 1 Master The Art Of Invisibility Bitcoins Hacking Kali Linux

Hiding Behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis exposes the latest electronic covert communication techniques used by cybercriminals, along with the needed investigative methods for identifying them. The book shows how to use the Internet for legitimate covert communication, while giving investigators the information they need for detecting cybercriminals who attempt to hide their true identity. Intended for practitioners and investigators, the book offers concrete examples on how to communicate securely, serving as an ideal reference for those who truly need protection, as well as those who investigate cybercriminals. Covers high-level strategies, what they can achieve, and how to implement them Shows discovery and mitigation methods using examples, court cases, and more Explores how social media sites and gaming technologies can be used for illicit communications activities Explores the currently in-use technologies such as TAILS and TOR that help with keeping anonymous online

Following the economic crisis of 2008, the website ' bitcoin.org ' was registered by a mysterious computer programmer called Satoshi Nakamoto. A new form of money was born: electronic cash. Does Bitcoin have the potential to change how the world transacts financially? Or is it just a passing fad, even a major scam? In Bitcoin: The Future of Money?, MoneyWeek ' s Dominic Frisby's explains this controversial new currency and how it came about, interviewing some of the key players in its development while casting light on its strange and murky origins, in particular the much-disputed identity of Nakamoto himself. Economic theory meets whodunnit mystery in this indispensable guide to one of the most divisive innovations of our time.

As a cybersecurity expert who presents on TV and at security conferences regularly, Scott Schober has seen an alarmingly disproportionate number of seniors being coerced, targeted, and robbed through the same internet we all share. From the basics of the internet to the fight for healthcare privacy and security that is so critical to our aging population, Senior Cyber offers simple advice and expertise for all levels of internet experience. Whether you are a parent, grandparent, great-grandparent, or the son or daughter of one, this book is designed with your concerns in mind. Practical cybersecurity advice and examples affecting seniors put Senior Cyber atop any reading list for those helping others or themselves to stay cyber safe. Basic tech and security topics: - email, browsers, search engines - big data pitfalls, privacy, security - healthcare cybersecurity - computer and smartphone basics - politics of technology - internet and phone scams to avoid - video chat in the age of COVID19 Advanced security topics: - spotting email phishing scams - dealing with spam and junk mail - creating strong passwords - keeping your searches private - avoiding big data collection - stopping identity theft before and after death - securing your digital footprint

Use This Information To Avoid Being Spied By The Government Today! If you've ever heard outrageous stories about online illegal drug stores, hit men for hire, celebrities busted for child porn, mad scientific experiments, and Illuminati rituals, you've probably heard of the "dark web", alternatively called the deep web. It's said to be the unchartered web browsing experience, the mysterious and sometimes terrifying "dark side" of the Internet, where you can supposedly find things that are shocking, illegal or highly top secret. It's a great story for sensationalist news magazines to tackle, especially when you have unconfirmed reports of aliens, cults, murders and other shocking things that no decent human being should ever see. It's also a favorite on YouTube horror and CreepyPasta, since they love adding onto urban legends. But have you ever wondered if these stories are true? What is the Deep Web or Dark Web, exactly? Here Is A Sneak Peek Of What You Will Learn What is the Deep Web and Why Is It Worth Exploring? Pros and Cons of Using Tor Pros and Cons of Proxies How to Avoid NSA Spying Anonymous Email What You Might Find on the Dark Market And Much Much More... Do Not Wait Any Longer And Get This Book For Only $13.38!

Hacking for Beginners
Tor and the Deep Web: Bitcoin, Darknet & Cryptocurrency (2 in 1 Book) 2017-18: Nsa Spying Defeated
Burners & Black Markets
Cult of the Dead Cow
Toward Proactive Cyber-Defense
Homeland
Web Scraping with Python

This extraordinary book explains the engine that has catapulted the Internet from backwater to ubiquity—and reveals that it is sputtering precisely because of its runaway success. With the unwitting help of its users, the generative Internet is on a path to a lockdown, ending its cycle of innovation—and facilitatin kinds of control. IPods, iPhones, Xboxes, and TiVos represent the first wave of Internet-centered products that can't be easily modified by anyone except their vendors or selected partners. These "tethered appliances" have already been used in remarkable but little-known ways: car GPS systems have been re demand of law enforcement to eavesdrop on the occupants at all times, and digital video recorders have been ordered to self-destruct thanks to a lawsuit against the manufacturer thousands of miles away. New Web 2.0 platforms like Google mash-ups and Facebook are rightly touted—but their applications ca monitored and eliminated from a central source. As tethered appliances and applications eclipse the PC, the very nature of the Internet—its "generativity," or innovative character—is at risk. The Internet's current trajectory is one of lost opportunity. Its salvation, Zittrain argues, lies in the hands of its millions of u generative technologies like Wikipedia that have so far survived their own successes, this book shows how to develop new technologies and social structures that allow users to work creatively and collaboratively, participate in solutions, and become true "netizens."

If you want to learn Linux programming, there

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 b 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 l 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) 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 hacke 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 a 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 vulnera 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 si 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 passw 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 hacking!Don't keep waiting to start your new journey as a hacker; get started now and order your copy today!

Kindle 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 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 a 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 g 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 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 M 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. H 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 th How to use Darkcoins 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 Ta 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 fi 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 those 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 wear a cloak of invisibility INSTANTLY!

Tor and the Dark Art of Anonymity
Hiding Behind the Keyboard
Tor Darknet
Darkest Web
The Complete Guide to Stay Anonymous in the Dark Net
Hacking with Kali Linux
Hacker, Hoaxer, Whistleblower, Spy

Kindle Anonymity Package - 3 Books for the Price of 1!Want a discounted price on THREE different eBooks?Here's what you'll get with this three book package:Darknet: The ULTIMATE Guide on HOW TO BE ANONYMOUS OnlineWas Snowden right? Want to surf the web anonymously? Cloak your activities? 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 private files, securing your PC, masking your online footsteps, and all while giving you peace of mind with TOTAL 100% ANONYMITY.Don't waste months scouring the internet for info. Read this instead. Much like J.J. Luna's How to Be Invisible, the pages turn themselves. - 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!You've probably read How to Be Invisible by J. J. Luna and How to Disappear by Frank Ahearn. While they are fine books, you need this companion piece to take it to the NEXT LEVEL. The pages turn themselves.Tor & The Dark Art of AnonymityThe 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 agentsThe Invisibility ToolkitYour sovereignty is under attack. You don't need the red pill to see it because you've already been unplugged. It's all around you.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.The Invisibility Toolkit is the ultimate guide for anyone who values their privacy or needs to disappear. Whether you're running from stalkers or hit men or overzealous cops or divorce courts, you owe it to yourself to learn how to protect your greatest asset: You and your family!But be warned. Going incognito is dangerous and for that you need a dangerous book. This book is one the NSA doesn't want you to read! It's stuff you won't see in any James Bond or Bourne film or even Burn Notice. But if you love freedom, this book is mandatory reading because it's life-saving reading. 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 Darkcoins on the Run- How to Sneak into Canada- How to Be Anonymous Online using Tor- Edward Snowden's biggest mistake.Download now and wear a cloak of invisibility TODAY!

So, You Are Interested In Being Anonymous Online... Look No Further! This book contains information vital for those who wish to surf the Internet anonymously.Before you read this book, ask yourself the following questions:How much do you know about the Tor Browser?How much do you know about the Dark Web and the Deep Web?Are you currently anonymous online?This book sets about informing you about these aspects in as simple a fashion as possible.This book does not confuse the reader with jargon and acronyms from computer science. It is authored for an intelligent layperson. You will learn a lot from it. Its contents should make you a bit worried.It will tell you about computer basics, general online safety, the Tor Browser, the Dark Web and the Deep Web.It tells you what to do if you want to surf the web like a hacker Here Is A Preview Of What You'll Learn... Protocols Are You Being Tracked Online? How To Stay Anonymous Online The Tor Browser Secrets Of The Dark Web How To Surf The Web Like A Hacker Much, much more! Download your copy today!

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.

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!

Beginning Ethical Hacking with Kali Linux
How to Be Anonymous Online With Tor, Bitcoin, Tails & More
Master the Art of Invisibility
Everything You Need to Know to Become an Elite Hacker
Hacking]
The Darknet Super-pack
Tor and the Deep Web

Open source intelligence (OSINT) and web reconnaissance are rich topics for infosec professionals looking for the best ways to sift through the abundance of information widely available online. In many cases, the first stage of any security assessment—that is, reconnaissance—is not given enough attention by security professionals, hackers, and penetration testers. Often, the information openly present is as critical as the confidential data. Hacking Web Intelligence shows you how to dig into the Web and uncover the information many don't even know exists. The book takes a holistic approach that is not only about using tools to find information online but also how to link all the information and transform it into presentable and actionable intelligence. You will also learn how to secure your information online to prevent it being discovered by these reconnaissance methods. Hacking Web Intelligence is an in-depth technical reference covering the methods and techniques you need to unearth open source information from the Internet and utilize it for the purpose of targeted attack during a security assessment. This book will introduce you to many new and leading-edge reconnaissance, information gathering, and open source intelligence methods and techniques, including metadata extraction tools, advanced search engines, advanced browsers, power searching methods, online anonymity tools such as TOR and i2p, OSINT tools such as Maltego, Shodan, Creepy, SearchDiggity, Recon-ng, Social Network Analysis (SNA), Darkweb/Deepweb, data visualization, and much more. Provides a holistic approach to OSINT and Web recon, showing you how to fit all the data together into actionable intelligence Focuses on hands-on tools such as TOR, i2p, Maltego, Shodan, Creepy, SearchDiggity, Recon-ng, FOCA, EXIF, Metagoofil, MAT, and many more Covers key technical topics such as metadata searching, advanced browsers and power searching, online anonymity, Darkweb / Deepweb, Social Network Analysis (SNA), and how to manage, analyze, and visualize the data you gather Includes hands-on technical examples and case studies, as well as a Python chapter that shows you how to create your own information-gathering tools and modify existing APIs

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.

Are you at risk of being scammed? Former con artist and bestselling author of Catch Me If You Can Frank Abagnale shows you how to stop scammers in their tracks. Maybe you're wondering how to make the scam phone calls stop. Perhaps someone has stolen your credit card number. Or you've been a victim of identity theft. Even if you haven't yet been the target of a crime, con artists are always out there, waiting for the right moment to steal your information, your money, and your life. As one of the world's most respected authorities on the subjects of fraud, forgery, and cyber security, Frank Abagnale knows how scammers work. In Scam Me If You Can, he reveals the latest tricks that today's scammers, hackers, and con artists use to steal your money and personal information--often online and over the phone. Using plain language and vivid examples, Abagnale reveals hundreds of tips, including: • The best way to protect your phone from being hacked • The only time you should ever use a debit card • The one type of photo you should never post on social media • The only conditions under which you should use WiFi networks at the airport • The safest way to use an ATM With his simple but counterintuitive rules, Abagnale also makes use of his insider intel to paint a picture of cybercrimes that haven't become widespread yet.

Would You Like to Learn Exactly What It Means to be a Hacker & How To Protect Your Identity On The Web? - NOW INCLUDES FREE GIFTS! (see below for details) Have you always secretly admired how tech savvy hackers are? Does the word "hacker" make you think of the cool kids who don''t obey society''s rules? Or does the idea of someone hacking your system and stealing your data make you break out into a cold sweat? Do you want to understand how hacking works for once and for all? Have you been drawn to the dark side of the web? Do you long for the days when anonymity on the web was the norm rather than the exception? Do you want to experience the web away from all prying eyes and experience real online freedom? Do you want to learn to play safely in the deep web? If the answer to any of these questions is yes, this book will provide you with the answers you''ve been looking for! In this book we''ll delve into the worlds of both Hacking and using Tor to stay anonymous. It might come as a surprise to you is that hacking does not need to mean having mad computer skills. You need to know some basics, naturally, but hacking a computer system is a lot simpler than you might think. And there are a lot of software and tools out there that can help you grow from a hacking novice to a hacking expert in a very short period of time. When it comes to Tor, the deep web, it''s one of the last true bastions of freedom on the internet. It is the place that few search engines dare to tread. It is exciting and has a true air of mystery about it. But it''s also a place that not too many people know how to access. Now I''m going to let you in on a secret - you can keep your anonymity on the web. You don''t have to know how to run elaborate software to delete all your tracks. All you need is a simple program. It''s free, it''s super-simple to install and run and you can use it today. TOR will do it all for you - it acts as an intermediary so that you don''t have to divulge your personal information when you are online. And then it routes your online activity through a number of different secure nodes making it really difficult to track. Could it really be that simple? Despite what you see in the movies, yes it can. But you do need to know the rules. You need to know how the system works and how to get it to work for you. This book is going to show you how to do that. You will learn how to make your first forays into the deep web. And hold your horses, it will be a fun ride.

The deep web is totally different from your normal internet. You need to know how to get it to give up its secrets. But, once you do, you will have a blast. In this book, we will look at: How Hacking Works Hacking Networks and Computer Systems Information Gathering Using the Data You Gathered Password Cracking for Beginners Applications to Gain Entry to Systems Wireless Hacking Staying Anonymous on the Deep Web What the TOR network is Whether or not TOR is the answer for you How to get started with TOR quickly and safely How to stay completely anonymous with TOR How to surf the dark web safely What you can expect to find on the dark web ...and much more! Also included for a limited time only are 2 FREE GIFTS, including a full length, surprise FREE BOOK! Take the first step towards becoming an expert hacker while maintaining complete online anonymity today. Click the buy now button above for instant access. Also included are 2 FREE GIFTS! - A sample from one of my other bestselling books, and a full length, FREE BOOK included with your purchase!

4 Books in 1- Hacking for Beginners, Hacker Basic Security, Networking Hacking, Kali Linux for Hackers

How to Be Invisible from Nsa Spying

Hacking Web Intelligence

Tor and the Dark Net

Server Security from TLS to Tor

3 Manuscripts - Bitcoin, Tor, Hacking with Python

The Dark Web Dive

Learn web scraping and crawling techniques to access unlimited data from any web source in any format. With this practical guide, you’ll learn how to use Python scripts and web APIs to gather and process data from thousands—or even millions—of web pages at once. Ideal for programmers, security professionals, and web administrators familiar with Python, this book not only teaches basic web scraping mechanics, but also delves into more advanced topics, such as analyzing raw data or using scrapers for frontend website testing. Code samples are available to help you understand the concepts in practice. Learn how to parse complicated HTML pages Traverse multiple pages and sites Get a general overview of APIs and how they work Learn several methods for storing the data you scrape Download, read, and extract data from documents Use tools and techniques to clean badly formatted data Read and write natural languages Crawl through forms and logins Understand how to scrape JavaScript Learn image processing and text recognition

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! Other books tell you to install Tor and then encrypt your hard drive... and leave it at that. I go much deeper, delving into the very engine of ultimate network security, taking it to an art form where you'll receive a new darknet persona - how to be anonymous online without looking like you're trying to be anonymous online. 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 - Which Offers Stronger Network Security? - Cryptocurrency (Real Bitcoin Anonymity) - Supercookies & Encryption - Preventing Marketers and Debt Collectors From Finding You - How to Protect Your Assets - i.e., How to Be Invisible and even Hide from the Internet itself! - How to Hide Anything Scroll back up and click "Look Inside" and Take Back Your Life Today!

D??? th? word "hacking" ???r? ??u? 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. G?n?r?ll?, h??k?ng has earned a n?g?t?v? r??ut?t??n ?nd h?? b???m? ???????t?d with ??b?r?tt??k? ?nd breaches ?n ??b?r???ur?t?. But this is not always tru?. If this is your f?r?t b??k on h??k?ng, ??u w?ll become m?r? acquainted w?th the w?rld ?f h??k?ng ?? th?? b??k g?v?? a simple overview ?f ethical hacking. Th? term "?th???l h??k?r" ?m?rg?d in th? l?t? 1970s wh?n th? US government h?r?d expert groups ??ll?d "red t??m?" t? hack their ?wn computer system. H??k?r? are ??b?r-?x??rt? who l?wfull? or ?ll?g?ll? h??k. Y?u enter the ???ur?t? ???t?m ?f a ??m?ut?r network to r?tr??v? ?r r???ll??t ?nf?rm?t??n. 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"!

The FBI wants to backdoor your smartphone. So does the NSA. They failed with Apple's iPhone but like most giants they'll try softer targets - targets that don't fight back. That's why unless you've got the proper tools to ward them off, they'll return like surveillance drones. Be ready for them. Buy this book and master anonymity and give the NSA a burn notice they'll never forget. A lot of books say install this, avoid that, but here you'll find easy steps to STARVE THE BEAST. No BS, No fluff, No Lame Theories, and No Sugar Coating. Just rock-solid tactical strategies for Tor, Tails & Burner Phones, field-tested and easy to understand. Read this to learn how to be invisible without LOOKING like you're trying to be invisible. Anywhere. Covered in Burners & Black Markets: - Best Burner Phones & Laptops - How to Be Anonymous on Android. Blackberry. iPhone. Laptops. - Cops & Cell Phones - Hacking Wireless - Online Privacy & Disaster Preparedness - Tor & Tails & Android - Anti-Hacker Tricks & The Latest Wireless Security Solutions - Buyer & Vendor Opsec for Black Markets - How to Protect Yourself from Scammers, Phishers & Identity Thieves Makes for an excellent companion piece to "How to Be Invisible" by J.J Luna & "How to Disappear" by Frank Ahearn. This book is REQUIRED READING if you want to learn the Dark Art of Anonymity! Scroll up and click "Look Inside" to get started!

Linux Hardening in Hostile Networks

Remain Anonymous and Evade Nsa Spying

The Many Faces of Anonymous

Linux: 5 Books in 1- Bible of 5 Manuscripts in 1- Beginner's Guide+ Tips and Tricks+ Effective Strategies+ Best Practices to

Computational Techniques for Resolving Security Issues

Exploring Malicious Hacker Communities

Darknet

An accessible introduction to cybersecurity concepts and practices Cybersecurity Essentials provides a comprehensive introduction to the field, with expert coverage of essential topics required for entry-level cybersecurity certifications. An effective defense consists of four distinct challenges: securing the infrastructure, securing devices, securing local networks, and securing the perimeter. Overcoming these challenges requires a detailed understanding of the concepts and practices within each realm. This book covers each challenge individually for greater depth of information, with real-world scenarios that show what vulnerabilities look like in everyday computing scenarios. Each part concludes with a summary of key concepts, review questions, and hands-on exercises, allowing you to test your understanding while exercising your new critical skills. Cybersecurity jobs range from basic configuration to advanced systems analysis and defense assessment. This book provides the foundational information you need to understand the basics of the field, identify your place within it, and start down the security certification path. Learn security and surveillance fundamentals Secure and protect remote access and devices Understand network topologies, protocols, and strategies Identify threats and mount an effective defense Cybersecurity Essentials gives you the building blocks for an entry level security certification and provides a foundation of cybersecurity knowledge

In Cory Doctorow's wildly successful Little Brother, young Marcus Yallow was arbitrarily detained and brutalized by the government in the wake of a terrorist attack on San Francisco—an experience that led him to become a leader of the whole movement of technologically clued-in teenagers, fighting back against the tyrannical security state. A few years later, California's economy collapses, but Marcus's hacktivist past lands him a job as webmaster for a crusading politician who promises reform. Soon his former nemesis Masha emerges from the political underground to gift him with a thumbdrive containing a Wikileaks-style cable-dump of hard evidence of corporate and governmental perfidy. It's incendiary stuff—and if Masha goes missing, Marcus is supposed to release it to the world. Then Marcus sees Masha being kidnapped by the same government agents who detained and tortured Marcus years earlier. Marcus can leak the archive Masha gave him—but he can't admit to being the leaker, because that will cost his employer the election. He's surrounded by friends who remember what he did a few years ago and regard him as a hacker hero. He can't even attend a demonstration without being dragged onstage and handed a mike. He's not at all sure that just dumping the archive onto the Internet, before he's gone through its millions of words, is the right thing to do. Meanwhile, people are beginning to shadow him, people who look like they're used to inflicting pain until they get the answers they want. Fast-moving, passionate, and as current as next week, Homeland is every bit the equal of Little Brother—a paean to activism, to courage, to the drive to make the world a better place. At the Publisher's request, this title is being sold without Digital Rights Management Software (DRM) applied.

Tor And The Deep Web: The Complete Guide To Stay Anonymous In The Dark Net Tor enables its users to surf the Internet, chat and send instant messages anonymously. Developed by the Tor Project, a nonprofit organization that promotes anonymity on the internet, Tor was originally called The Onion Router due to the fact that it uses a technique called "onion routing" to hide information about user activity. With this book you can learn about: -Introduction to Tor -Installing the Tor browser -How to use tor to protect your privacy -5 important facts you need to know -Legal or illegal -Tips & recommendations And much, much more!

Do you want to learn how to use Python to Hack? Do you want to learn how to conceal your IP Address and block NSA Spying? Do you want to learn how to invest in the revolutionary cryptocurrency that is Bitcoin? If you answered yes, then this book is right for you! The simple term -Bitcoin- can be intimidating to some people, especially those who have never purchased a Bitcoin or have ever dealt in the currency before. There are many options when it comes to Bitcoin, and you need to make sure that you are getting the most out of the investment process. Anyone who is considering investing in Bitcoin should take their time and learn as much about it as possible. The actual act of purchasing a Bitcoin can be lengthy and can cost you a lot of money so make sure that you are as well informed as possible. As one of the best and most mysterious investment opportunities, learn more about Bitcoin. The Internet is a wonderful resource which has allowed people to access a fountain of knowledge with the simple click of a button. The internet has grown considerably fast in the last decade, and it is still expanding at extraordinary rates. But with this incredible tool comes a danger! The government has been using our vast resource to spy on individuals and businesses, overstepping their role as an entity that exists to serve the people. In this book, you will learn how to fight back against the government and NSA. You will also discover how you can browse online while remaining anonymous. In addition to getting all of this information, you will also learn how to hack with Python! You will discover all types of hacking from ethical hacking to black hat hacking. Whether you are a hacking novice or hacking maestro, you will love these books! What does this book bundle include? Amazon No. 1 Bestseller - Bitcoin Amazon No. 1 Bestseller - Tor Hacking With Python 3 - BOOKS 2 - #1 Bestsellers! Tags: python, python for beginners, python programming, python programming for beginners, python language, learn python, python 3, python crash course, hacking, hack, learn how to hack, how to hack, hacking university, hacking for beginners, black hat, gray hat, grey hat, white hat, tor, deep web, dark web, deep net, dark net, darknet, bitcoin, blockchain, investing, money, how to make money, bitcoin trading, bitcoin mining, blockchain blueprint

The Pentester BluePrint

Open Source Intelligence and Web Reconnaissance Concepts and Techniques

Tor

Kali Linux Social Engineering

Uncovering Covert Communication Methods with Forensic Analysis

Scam Me If You Can

Hitmen for Hire, Drugs for Sale. Inside the Dangerous World That Lurks Beneath the Bright, Friendly Light of Your Internet Screen

Inside the Dark Web provides a broad overview of emerging digital threats and computer crimes, with an emphasis on cyberstalking, hacktivism, fraud and identity theft, and attacks on critical infrastructure. The book also analyzes the online underground economy and digital currencies and cybercrime on the dark web. The book further explores how dark web crimes are conducted on the surface web in new mediums, such as the Internet of Things (IoT) and peer-to-peer file sharing systems as well as dark web forensics and mitigating techniques. This book starts with the fundamentals of the dark web along with explaining its threat landscape. The book then introduces the Tor browser, which is used to access the dark web ecosystem. The book continues to take a deep dive into cybersecurity criminal activities in the dark net and analyzes the malpractices used to secure your system. Furthermore, the book digs deeper into the forensics of dark web, web content analysis, threat intelligence, IoT, crypto market, and cryptocurrencies. This book is a comprehensive guide for those who want to understand the dark web quickly. After reading Inside the Dark Web, you’ll understand The core concepts of the dark web. The different theoretical and cross-disciplinary approaches of the dark web and its evolution in the context of emerging crime threats. The forms of cybercriminal activity through the dark web and the technological and "social engineering" methods used to undertake such crimes. The behavior and role of offenders and victims in the dark web and analyze and assess the impact of cybercrime and the effectiveness of their mitigating techniques on the various domains. How to mitigate cyberattacks happening through the dark web. The dark web ecosystem with cutting edge areas like IoT, forensics, and threat intelligence and so on. The dark web-related research and applications and up-to-date on the latest technologies and research findings in this area. For all present and aspiring cybersecurity professionals who want to upgrade their skills by understanding the concepts of the dark web, Inside the Dark Web is their one-stop guide to understanding the dark web and building a cybersecurity plan.

-- 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?

Here is the ultimate book on the worldwide movement of hackers, pranksters, and activists that operates under the non-name Anonymous, by the writer the Huffington Post says “knows all of Anonymous’ deepest, darkest secrets.” Half a dozen years ago, anthropologist Gabriella Coleman set out to study the rise of this global phenomenon just as some of its members were turning to political protest and dangerous disruption (before Anonymous shot to fame as a key player in the battles over WikiLeaks, the Arab Spring, and Occupy Wall Street). She ended up becoming so closely connected to Anonymous that the tricky story of her inside–outside status as Anon confidante, interpreter, and erstwhile mouthpiece forms one of the themes of this witty and entirely engrossing book. The narrative brims with details unearthed from within a notoriously mysterious subculture, whose semi-legendary tricksters—such as Topiary, tflow, Anachaos, and Sabu—emerge as complex, diverse, politically and culturally sophisticated people. Propelled by years of chats and encounters with a multitude of hackers, including imprisoned activist Jeremy Hammond and the double agent who helped put him away, Hector Monsegur, Hacker, Hoaxer, Whistleblower, Spy is filled with insights into the meaning of digital activism and little understood facets of culture in the Internet age, including the history of “trolling,” the ethics and metaphysics of hacking, and the origins and manifold meanings of “the lulz.”

THE ULTIMATE TOR BROWSER & DARKNET GUIDE FOR 2018-2019Just three questions you need to ask yourself:✓ Do You Value Privacy?✓ Do You Value Freedom?✓ Do You Want to be Anonymous?If you answered yes to any of the above, then this is your book. Instant anonymity, right now, can be yours for the taking. As science fiction author Hugh Howey once stated: When Pursuing a Dream, Don't Wait.People sling words across the internet without regard for their future. They don't know it but they are digging their own graves by attacking Goliath without a shield. Every word you say on forums, Usenet, Facebook,and News outlets is out there forever whether you are Republican, Democrat, Libertarian or Green Party. Doesn't matter. One day you may wake up to discover a state power wants a 'type' of voter out of the equation altogether: You.How do you erase every critical forum comment you ever made?How do you scrub your Facebook page?How do you make anonymous online comments so that your new employer doesn't fire you?Enter Tor.This is the ultimate guide with easy take-you-by-the-hand instructions to teach you not only Tor, but VPNs, Bitcoins, Hacking, Darknet Personas and even how to evade the Sauronic Eye that is the NSA. Yes. This book kills NSA spying dead.✓ Comment Anonymously on ANY Website✓ Tor Browser, Freenet, I2P, and ALL Alternatives✓ Cryptocurrency - How to Buy\Sell Anonymously✓ Encryption Guide: PGP. Veracrypt. Email. Linux. Windows. Macs. Kali. Android. Phones.✓ Online Privacy No Matter Where You Are✓ Hacking Guide for Beginners on the Darknet✓ Edward Snowden's Biggest MistakeMaster the Art of Invisibility TODAY by scrolling up and hitting the BUY now button!

Ethical Hacking and Cybersecurity

Best Security Practices for Your Golden Years

Bitcoin

Hacking

Tor Browser

3 Books in 1: A Beginners Guide for Hackers (How to Hack Websites, Smartphones, Wireless Networks) + Linux Basic for Hackers (Command Line and All the Essentials) + Hacking with Kali Linux

How the Original Hacking Supergroup Might Just Save the World

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.

Dark... A kingpin willing to murder to protect his dark web drug empire. A corrupt government official determined to avoid exposure. The death of a dark web drugs czar in mysterious circumstances in a Bangkok jail cell, just as the author arrives there. Who is Variety Jones and why have darknet markets ballooned tenfold since authorities shut down the original dark web drugs bazaar, Silk Road? Who are the kingpins willing to sell poisons and weapons, identities and bank accounts, malware and life-ruining services online to anyone with a wallet full of Bitcoin? Darker... A death in Minnesota leads detectives into the world of dark web murder-for-hire where hundreds of thousands of dollars in Bitcoin is paid to arrange killings, beatings and rapes. Meanwhile, the owner of the most successful hitman website in history is threatening the journalists who investigate his business with a visit from his operatives - and the author is at the top of his list. Darkest... People with the most depraved perversions gather to share their obscene materials in an almost inaccessible corner of the dark web. A video circulates and the pursuit of the monsters responsible for 'Daisy's Destruction' lead detectives into the unimaginable horror of the world of hurtcore. There's the world wide web - the internet we all know that connects us via news, email, forums, shopping and social media. Then there's the dark web - the parallel internet accessed by only a select few. Usually, those it connects wish to remain anonymous and for good reason. 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.

Welcome to the wonderful world of hacking, a seemingly magical world, crafted out of the heart of mystery and wonder, but an oh so very real world where those who hesitate for even just a moment end up in very deep doo-doo, and only the elite have what it takes to survive!

Want to surf the web anonymously? This book is the perfect guide for anyone who wants to cloak their online activities. Whether you're on Usenet, Facebook, P2P, or browsing the web with standard browsers like Opera, Firefox and Internet Explorer, I will show you how to become a ghost on the internet, leaving no tracks back to your isp, or anyone else. This book covers every facet of encrypting your private data, securing your pc, masking your online footsteps, and gives you peace of mind with TOTAL 100% ANONYMITY on the internet. - Learn how to mask your online identity with *every* site or protocol you use online - In depth guides on Tor, Freenet, I2P, Proxies, VPNs, Usenet and much, much, more! - Learn about basic mistakes that even advanced hackers make every day that give them away - Learn which programs make you a ghost on the internet, and which shine the spotlight on you! - Get 100% security with online *and* offline computer habits! Regardless of what you do online, you owe it to yourself to make sure you aren't taken advantage of!

Web Penetration Testing with Kali Linux
A Beginner's Guide to Learn Penetration Testing to Protect Your Family and Business from Cyber Attacks Building a Home Security System for Wireless Network Security
How to Be Invisible
Access the Dark Net, Stay Anonymous Online and Escape Nsa Spying
The Future of the Internet--And How to Stop It
Starting a Career as an Ethical Hacker
A Beginner's Guide to Understand Cyber Security and Ethical Hacking. Protect Your Business and Your Family from Cybercrime

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.

This book is a practical, hands-on guide to learning and performing SET attacks with multiple examples.Kali Linux Social Engineering is for penetration testers who want to use BackTrack in order to test for social engineering vulnerabilities or for those who wish to master the art of social engineering attacks.

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.

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.

The Future of Money?
A Beginner's Guide to Staying Anonymous Online
Legitimacy on Freenet, Tor, and I2P
Hacking & Tor
Inside the Dark Web
Senior Cyber
The Ultimate Beginners Guide to Hacking, Tor, & Accessing the Deep Web & Dark Web

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!

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

Collecting Data from the Modern Web
Weaving the Dark Web
Simple Strategies to Outsmart Today's Rip-off Artists
Learn to Avoid Nsa Spying and Become Anonymous Online
Secrets of the Deep Web, How to Stay Anonymous Online, and Surf the Web Like a Hacker
A Complete Guide to The Dark Web
Cybersecurity Essentials