Introduction

Aside from white papers, blogs, podcasts and videos, books are a great resource for developing new skills and gaining knowledge in cyber security. Thankfully, you've a multitude to choose from, particularly if you're interested in penetration testing, hacking security research and exploit development.

Whilst many books are available, remember no one book covers all the skills and knowledge you'll need to be an expert in cyber security. The area is extremely diverse and as a result your study will need to be on-going if you want to become an expert.

The books that are listed here are community driven as nothing beats a good recommendation. They range from study guides to novels and from beginner level to advanced. They have been roughly grouped into the following categories:

- Study guides for certifications
- Computer security and secure networking
- Penetration testing
- Social engineering
- Secure coding
- Risk
- Incident response
- Secure Operating Centres
- Forensics
- Cryptography
- Novels

In addition to these books, you can also try the ISACA website / bookstore as it has significant materials related to security especially COBIT security related books, CISM manuals, CISA manuals and so on. Some are free, some are open to ISACA members-only and others you'll have to purchase. Finally, when you attend OWASP, ISACA or (ISC)² local meetings ask the members for their opinions on good books.
CISSP All-in-One Exam Guide, 6th Edition - fully revised for the latest release of the Certified Information Systems Security Professional exam, this comprehensive, up-to-date resource covers all 10 CISSP exam domains developed by the International Information Systems Security Certification Consortium (ISC)². This authoritative exam guide features learning objectives at the beginning of each chapter, exam tips, practice questions, and in-depth explanations.

Author: Shon Harris  
Series: All-in-One  
Hardcover: 1456 pages  
Language: English  
ISBN-10: 0071781749  

CISSP Practice Exams, Third Edition - fully updated throughout and featuring new question types, this self-study tool contains more than 1250 realistic practice exam questions covering all 10 CISSP exam domains developed by the International Information Systems Security Certification Consortium (ISC)².

To aid in your understanding of the material, in-depth explanations of both the correct and incorrect answers are provided for every question. Designed to help you pass the exam, this is the perfect companion to CISSP All-in-One Exam Guide.

Author: Shon Harris  
Paperback: 480 pages  
Publisher: McGraw-Hill Education; 3rd edition (March 2, 2015)  
Language: English  
ISBN-10: 0071845429  

CISSP Practice Exams, Fourth Edition - (due Aug 2016) fully updated and featuring new exam question formats, this self-study tool contains more than 1250 realistic practice exam questions and offers 100% coverage of the 2015 CISSP Common Body of Knowledge. In-depth explanations of both the correct and incorrect answers are provided for every question. This book is the perfect companion to CISSP All-in-One Exam Guide, Seventh Edition.

Designed as an exam-focused self-study aid and resource, CISSP Practice Exams, Fourth Edition, fully covers the eight newly-revised exam domains. The logical structure of the book
allows you to focus on specific topics and tailor your study to areas of expertise and weakness. Each chapter presents more than 25 examination questions—an additional 1000+ review questions are contained in the book's electronic content.

Authors: Shon Harris, Jonathan Ham
Paperback: 580 pages
Publisher: McGraw-Hill Education; 4th edition (August 22, 2016)
Language: English
ISBN-10: 1259585964

**Wireshark Essentials** - This book introduces the Wireshark network analyzer to IT professionals across multiple disciplines. It starts off with the installation of Wireshark, before gradually taking you through your first packet capture, identifying and filtering out just the packets of interest, and saving them to a new file for later analysis. The subsequent chapters will build on this foundation by covering essential topics on the application of the right Wireshark features for analysis, network protocols essentials, troubleshooting, and analyzing performance issues. Finally, the book focuses on packet analysis for security tasks, command-line utilities, and tools that manage trace files.

Upon finishing this book, you will have successfully added strong Wireshark skills to your technical toolset and significantly increased your value as an IT professional.

Author: James Baxtor
Paperback: 194 pages
Publisher: Packt Publishing - ebooks Account (October 28, 2014)
Language: English
ISBN-10: 1783554630

**Wireshark 101: Essential Skills for Network Analysis (Wireshark Solutions)** - this book is written for beginner analysts and includes 46 step-by-step labs to walk you through many of the essential skills contained herein. This book provides an ideal starting point whether you are interested in analyzing traffic to learn how an application works, you need to troubleshoot slow network performance, or determine whether a machine is infected with malware.

Learning to capture and analyze communications with Wireshark will help you really understand how TCP/IP networks function. As the most popular network analyzer tool in the world, the time you spend honing your skills with Wireshark will pay off when you read technical specs, marketing materials, security briefings, and more. This book can also be used by current analysts who need to practice the skills contained in this book. In essence,
this book is for anyone who really wants to know what's happening on their network.

Author: Laura Chappell  
Series: Wireshark Solutions  
Paperback: 370 pages  
Publisher: Laura Chappell University (February 1, 2013)  
Language: English  
ISBN-10: 1893939723  

Troubleshooting with Wireshark: Locate the Source of Performance Problems – whether you are a Wireshark newbie or an experienced Wireshark user, this book streamlines troubleshooting techniques used by Laura Chappell in her 20+ years of network analysis experience. This book consists of troubleshooting labs to walk you through the process of measuring client/server/network delays, detecting application error responses, catching delayed responses, locating the point of packet loss, spotting TCP receiver congestion, and more.

Key topics include: path delays, client delays, server delays, connection refusals, service refusals, receive buffer overload, rate throttling, packet loss, redirections, queueing along a path, resolution failures, small MTU sizes, port number reuse, missing support for TCP SACK/Window Scaling, misbehaving infrastructure devices, weak signals (WLAN), and more.

Author: Laura Chappell  
Paperback: 408 pages  
Publisher: Laura Chappell University (January 19, 2014)  
Language: English  
ISBN-10: 1893939979  

The Official Wireshark Certified Network Analyst Study Guide - this book is the Official Study Guide for the Wireshark Certified Network Analyst program. Wireshark is the world's most popular network analyzer tool with over 500,000 downloads per month. This book provides insider tips and tricks to spot performance issues fast - no more finger pointing because the packets never lie! From "Death by Database" to "Troubleshooting Time Syncing," 49 case studies offer insight into performance and security situations solved with Wireshark.

Learn to customize Wireshark for faster and more accurate analysis of your network traffic. Build graphs to identify and expose issues such as packet loss, receiver congestion, slow
server response, network queuing and more. This Second Edition includes an introduction to IPv6, ICMPv6 and DHCPv6 analysis, updated Wireshark functionality and new trace files. Refer to wiresharkbook.com for book supplements, index, table of contents and more.

Author: Laura Chappell
Paperback: 986 pages
Publisher: Laura Chappell University; 2nd edition (March 1, 2012)
Language: English
ISBN-10: 1893939944

CompTIA Security+: Get Certified Get Ahead: SY0-401 Study Guide - is an update to the top-selling SY0-201 and SY0-301 study guides, which have helped thousands of readers pass the exam the first time they took it. After a comprehensive review by ProCert Labs, the SY0-401 version has been certified as CompTIA Approved Quality Content (CAQC) and covers every aspect of the SY0-401 exam.

It includes the same elements readers raved about in the previous two versions. Each of the eleven chapters presents topics in an easy to understand manner and includes real-world examples of security principles in action. The author uses many of the same analogies and explanations he’s honed in the classroom that have helped hundreds of students master the Security+ content.

You’ll understand the important and relevant security topics for the Security+ exam, without being overloaded with unnecessary details. Additionally, each chapter includes a comprehensive review section to help you focus on what’s important.

Over 400 realistic practice test questions with in-depth explanations will help you test your comprehension and readiness for the exam. The book includes a 100 question pre-test, a 100 question post-test, and practice test questions at the end of every chapter. Each practice test question includes a detailed explanation to help you understand the content and the reasoning behind the question. You’ll be ready to take and pass the exam the first time you take it.

Author: Darril Gibson
Paperback: 560 pages
Publisher: YCDA, LLC; 3rd edition (October 25, 2014)
Language: English
ISBN-10: 1939136024
CompTIA Security+ Get Certified Get Ahead: SY0-401 Practice Test Questions - includes 307 realistic practice test questions with in-depth explanations. If you want to test your readiness for the Security+ (SY0-401) exam and reinforce the important material, this book is for you. It is organized in six chapters aligned with the six Security+ domains.

Author: Darril Gibson
Paperback: 360 pages
Publisher: YCDA, LLC; 2nd edition (December 19, 2014)
Language: English
ISBN-10: 1939136032

CompTIA Security+ Certification Practice Exams, Second Edition (Exam SY0-401) (Certification Press) 2nd Edition – is filled with more than 800 realistic practice questions—including new performance-based questions—to prepare you for this challenging exam. To help you understand the material, in-depth explanations of both the correct and incorrect answers are included for every question. This practical guide covers all official objectives for Exam SY0-401 and is the perfect companion to CompTIA Security+ Certification Study Guide, Second Edition.

Authors: Daniel Lachance, Glen E. Clarke
Series: Certification Press
Paperback: 384 pages
Publisher: McGraw-Hill Education; 2nd edition (July 9, 2014)
Language: English
ISBN-10: 0071833447


Cutting-edge coverage of the new edition includes virtualization, mobile devices, and other trends, as well as new topics such as psychological approaches to social engineering attacks, Web application attacks, penetration testing, data loss prevention, cloud computing security, and application programming development security.
Computer Networks: A Systems Approach – this best-selling and classic book teaches you the key principles of computer networks with examples drawn from the real world of network and protocol design. Using the internet as the primary example, the authors explain various protocols and networking technologies. Their systems-oriented approach encourages you to think about how individual network components fit into a larger, complex system of interactions.

Key features completely updated content with expanded coverage of the topics of utmost importance to networking professionals and students, including p2p, wireless, security, and applications. Increased focus on application layer issues where innovative and exciting research and design is currently the center of attention. Free downloadable network simulation software and lab experiments manual available.

Authors: Larry L Peterson and Bruce S Davie
Paperback
Publisher: TBS (2011)
Language: English
ISBN-10: 9380501935

Dynamics of a Trusted Platform – security threats are increasing in volume, diversity, and sophistication at the same time that high-value, sensitive data is more commonly being generated, used, and stored on standard business PCs. While the traditional focus of network protection has been on servers and network access devices, these PCs are typically lightly protected, coupled with the fact that a compromised PC may offer the means to obtain access to servers and other network assets, these characteristics have created an incentive for hackers to focus their efforts on client computing platforms.

Author: David Grawrock and Andrew Martin (Foreward)
Paperback: 450 pages
Publisher: Intel Press (2009)
Language: English
ISBN-10: 1934053082
Computer Architecture: A Quantitative Approach – The computing world today is in the middle of a revolution: mobile clients and cloud computing have emerged as the dominant paradigms driving programming and hardware innovation today. The fifth edition of Computer Architecture focuses on this dramatic shift, exploring the ways in which software and technology in the cloud are accessed by cell phones, tablets, laptops, and other mobile computing devices. Each chapter includes two real-world examples, one mobile and one data center, to illustrate this revolutionary change.

Authors: John L Hennessy and David A. Patterson
Series: The Morgan Kaufmann Series in Computer Architecture and Design
Paperback: 856 pages
Publisher: Morgan Kaufmann; 5th edition (September 30, 2011)
Language: English
ISBN-10: 012383872X

Modern Operating Systems – is intended for introductory courses in Operating Systems in Computer Science, Computer Engineering, and Electrical Engineering programs. The widely anticipated revision of this worldwide bestseller incorporates the latest developments in operating systems (OS) technologies. The Fourth Edition includes up-to-date materials on relevant OS. Tanenbaum also provides information on current research based on his experience as an operating systems researcher.

Author: Morgan Kaufmann
Paperback
Publisher: Pearson Education Limited; 4th Revised edition
Language: English
ISBN-10: 1292061421

Computer Security – assuming no previous experience in the field of computer security, this must-have book walks you through the many essential aspects of this vast topic, from the newest advances in software and technology to the most recent information on Web applications security.

This new edition includes sections on Windows NT, CORBA, and Java and discusses cross-site scripting and JavaScript hacking as well as SQL injection. Serving as a helpful introduction, this self-study guide is a wonderful starting point for examining the variety of competing security systems and what makes them different from one another.
Network Security – the comprehensive A-to-Z guide on network security, fully revised and updated. Network security is constantly evolving, and this comprehensive guide has been thoroughly updated to cover the newest developments. If you are responsible for network security, this is the reference you need at your side. Covering new techniques, technology, and methods for approaching security, it also examines new trends and best practices being used by many organizations. The revised Network Security Bible complements the Cisco Academy course instruction in networking security.

Computer Networks and Internets – Appropriate for all introductory-to-intermediate courses in computer networking, the Internet, or Internet applications; readers need no background in networking, operating systems, or advanced mathematics.

Leading networking authority Douglas Comer presents a wide-ranging, self-contained tour of the concepts, principles, and technologies that enable today’s Internet to support applications ranging from web browsing to telephony and multimedia. Comer begins by illuminating the applications and facilities offered by today’s Internet. Next, he systematically introduces the underlying network technologies and protocols that make them possible. With these concepts and technologies established, he introduces several of the most important contemporary issues faced by network implementers and managers, including quality of service, Internet telephony, multimedia, network security, and network management.

Comer has carefully designed this book to support both top-down and bottom-up teaching approaches. Students need no background in operating systems, and no sophisticated math: Comer relies throughout on figures, drawings, examples, and analogies, not mathematical proofs.
Author: Douglas Comer
Paperback
Publisher: Pearson Education Limited; 6th edition
Language: English
ISBN-10: 1292061170

**Network Intrusion Detection, 3rd Edition** – The Chief Information Warfare Officer for the entire United States teaches you how to protect your corporate network. This book is a training aid and reference for intrusion detection analysts. While the authors refer to research and theory, they focus their attention on providing practical information. The authors are literally the most recognized names in this specialized field, with unparalleled experience in defending our country's government and military computer networks. New to this edition is coverage of packet dissection, IP datagram fields, forensics, and snort filters.

Authors: Stephen Northcutt and Judy Novak
Paperback: 512 pages
Publisher: Sams Publishing; 3rd edition (September 6, 2002)
Language: English
ISBN-10: 0735712654

**The Art of Intrusion** – Kevin Mitnick, is the world's most celebrated hacker and now devotes his life to helping businesses and governments combat data thieves, cybervandals, and other malicious computer intruders. In his bestselling The Art of Deception, Mitnick presented fictionalized case studies that illustrated how savvy computer crackers use "social engineering" to compromise even the most technically secure computer systems. Now, in his new book, Mitnick goes one step further, offering hair–raising stories of real–life computer break–ins and showing how the victims could have prevented them.

Author: Kevin Mitnick
Hardcover: 290 pages
Publisher: John Wiley & Sons; 1st edition (18 Feb. 2005)
Language: English
ISBN-10: 0764569597

**Ghost in the Wires** – Kevin Mitnick, the world's most wanted computer hacker, managed to hack into some of the country's most powerful - and seemingly impenetrable - agencies and
companies. By conning employees into giving him private information and manoeuvring through layers of security, he gained access to data that no one else could.

The suspenseful heart of the book unfolds as Mitnick disappears on a three-year run from the FBI. He creates fake identities, finds jobs at a law firm and hospital, and keeps tabs on his myriad pursuers - all while continuing to hack into computer systems and phone company switches that were considered flawless.

A modern, technology-driven adventure story, GHOST IN THE WIRES is a dramatic account of the joy of outsmarting security programs, the satisfaction of code-cracking, and the thrill of unbelievable escape.

Author: Kevin Mitnick
Paperback: 560 pages
Publisher: Back Bay (3 May 2012)
Language: English
ISBN-10: 0316212180

The Future Crimes - technological advances have benefited our world in immeasurable ways, but there is an ominous flipside. Criminals are often the earliest, and most innovative, adopters of technology and modern times have led to modern crimes. Today's criminals are stealing identities, draining online bank accounts and wiping out computer servers. It's disturbingly easy to activate baby cam monitors to spy on families, pacemakers can be hacked to deliver a lethal jolt, and thieves are analyzing your social media in order to determine the best time for a home invasion.

Meanwhile, 3D printers produce AK-47s, terrorists can download the recipe for the Ebola virus, and drug cartels are building drones. This is just the beginning of the tsunami of technological threats coming our way. In Future Crimes, Marc Goodman rips open his database of hundreds of real cases to give us front-row access to these impending perils. Reading like a sci-fi thriller, but based in startling fact, Goodman raises tough questions about the expanding role of technology in our lives. Future Crimes is a call to action for better security measures worldwide, but most importantly, will empower readers to protect themselves against these looming technological threats - before it's too late.

Author: Marc Goodman
Hardcover: 464 pages
Publisher: Bantam Press (26 Feb. 2015)
Language: English
ISBN-10: 0593073657
Beautiful Security: Leading Security Experts Explain How They Think – although most people don't give security much attention until their personal or business systems are attacked, this thought-provoking anthology demonstrates that digital security is not only worth thinking about, it's also a fascinating topic. Criminals succeed by exercising enormous creativity, and those defending against them must do the same.

Authors: Andy Oram and John Viega
Paperback: 302 pages
Publisher: O'Reilly Media; 1 edition (8 May 2009)
Language: English
ISBN-10: 0596527489

Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door - In Spam Nation, investigative journalist and cybersecurity expert Brian Krebs unmasksthe criminal masterminds driving some of the biggest spam and hacker operations targeting Americans and their bank accounts. Tracing the rise, fall, and alarming resurrection of the digital mafia behind the two largest spam pharmacies-and countless viruses, phishing, and spyware attacks-he delivers the first definitive narrative of the global spam problem and its threat to consumers everywhere.

Blending cutting-edge research, investigative reporting, and first-hand interviews, this terrifying true story reveals how we unwittingly invite these digital thieves into our lives every day. From unassuming computer programmers right next door to digital mobsters like "Cosma"-who unleashed a massive malware attack that has stolen thousands of Americans' logins and passwords-Krebs uncovers the shocking lengths to which these people will go to profit from our data and our wallets.

Not only are hundreds of thousands of Americans exposing themselves to fraud and dangerously toxic products from rogue online pharmacies, but even those who never open junk messages are at risk. As Krebs notes, spammers can-and do-hack into accounts through these emails, harvest personal information like usernames and passwords, and sell them on the digital black market. The fallout from this global epidemic doesn't just cost consumers and companies billions, it costs lives too.

Fast-paced and utterly gripping, Spam Nation ultimately proposes concrete solutions for protecting ourselves online and stemming this tidal wave of cybercrime-before it's too late.
Visible Ops Security: Achieving Common Security And IT Operations Objectives In 4 Practical Steps - this second edition leverages the four phases laid out in the first edition, taking into account the state of today’s IT environment. The core concepts are just as valid today as they were five years ago. Scott Alldridge, President, IT Process Institute Visible Ops Security addresses the people side of IT, empowering security to work with operations teams to achieve closely aligned objectives and with development and release teams to integrate security requirements into pre-production work. The Visible Ops Security methodology helps IT organizations move beyond a focus on technology to address the core operational aspects of security. It promotes effective teamwork, which helps security professionals ensure that security is built into key development and production processes.

Authors: Gene Kim, Paul Love, George Spafford
Paperback: 111 pages
Publisher: IT Process Institute Inc.; Second edition (October 15, 2014)
Language: English
ISBN-10: 097556868X

The Tao of Network Security Monitoring: Beyond Intrusion Detection - Richard Bejtlich explores the products, people, and processes that implement the NSM model. By focusing on case studies and the application of open source tools, he helps you gain hands-on knowledge of how to better defend networks and how to mitigate damage from security incidents.

Author: Richard Bejtlich
Paperback: 832 pages
Publisher: Addison-Wesley Professional; 1 edition (July 22, 2004)
Language: English
ISBN-10: 0321246772

Inside Network Perimeter Security – Security professionals and administrators now have access to one of the most valuable resources for learning best practices for network perimeter security. *Inside Network Perimeter Security, Second Edition* is your guide to
preventing network intrusions and defending against any intrusions that do manage to slip through your perimeter. This acclaimed resource has been updated to reflect changes in the security landscape, both in terms of vulnerabilities and defensive tools. Coverage also includes intrusion prevention systems and wireless security. You will work your way through fortifying the perimeter, designing a secure network, and maintaining and monitoring the security of the network. Additionally, discussion of tools such as firewalls, virtual private networks, routers and intrusion detection systems make Inside Network Perimeter Security, Second Edition a valuable resource for both security professionals and GIAC Certified Firewall Analyst certification exam candidates.

Authors: Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey
Paperback: 768 pages
Publisher: Sams Publishing; 2nd edition (March 14, 2005)
Language: English
ISBN-10: 0672327376

Botnets: The Killer Web App – the book begins with real world cases of botnet attacks to underscore the need for action. Next the book will explain botnet fundamentals using real world examples. These chapters will cover what they are, how they operate, and the environment and technology that makes them possible. The following chapters will analyze botnets for opportunities to detect, track, and remove them. Then the book will describe intelligence gathering efforts and results obtained to date. Public domain tools like OurMon, developed by Jim Binkley of Portland State University, will be described in detail along with discussions of other tools and resources that are useful in the fight against Botnets.

Authors: Craig Schiller, Jim Binkley, Gadi Evron
Paperback: 480 pages
Publisher: Syngress; 1st edition (February 15, 2007)
Language: English
ISBN-10: 1597491357

Counter Hack Reloaded: A Step-by Step Guide to Computer Attacks and Effective Defenses (2nd Edition) – for years, Counter Hack has been the primary resource for every network/system administrator and security professional who needs a deep, hands-on understanding of hacker attacks and countermeasures. Now, leading network security expert Ed Skoudis, with Tom Liston, has thoroughly updated this best-selling guide, showing how to defeat today's newest, most sophisticated, and most destructive attacks.
For this second edition, more than half the content is new and updated, including coverage of the latest hacker techniques for scanning networks, gaining and maintaining access, and preventing detection. The authors walk you through each attack and demystify every tool and tactic. You'll learn exactly how to establish effective defenses, recognize attacks in progress, and respond quickly and effectively in both UNIX/Linux and Windows environments.

Authors: Edward Skoudis, Tom Liston
Paperback: 748 pages
Publisher: Prentice Hall; 2nd edition (January 2, 2006)
Language: English
ISBN-10: 0131481045

**Extrusion Detection** – is a comprehensive guide to preventing, detecting, and mitigating security breaches from the inside out. Top security consultant Richard Bejtlich offers clear, easy-to-understand explanations of today's client-based threats and effective, step-by-step solutions, demonstrated against real traffic and data. You will learn how to assess threats from internal clients, instrument networks to detect anomalies in outgoing traffic, architect networks to resist internal attacks, and respond effectively when attacks occur.

Bejtlich's *The Tao of Network Security Monitoring* earned acclaim as the definitive guide to overcoming external threats. Now, in Extrusion Detection, he brings the same level of insight to defending against today's rapidly emerging internal threats. Whether you're an architect, analyst, engineer, administrator, or IT manager, you face a new generation of security risks. Get this book and protect yourself.

Author: Richard Bejtlich
Paperback: 416 pages
Publisher: Addison-Wesley Professional (November 18, 2005)
Language: English
ISBN-10: 0321349962

**Google Hacking for Penetration Testers** – Google is the most popular search engine ever created, but Google's search capabilities are so powerful, they sometimes discover content that no one ever intended to be publicly available on the Web, including social security numbers, credit card numbers, trade secrets, and federally classified documents. Google Hacking for Penetration Testers, Third Edition, shows you how security professionals and system administrators manipulate Google to find this sensitive information and "self-police" their own organizations.
You will learn how Google Maps and Google Earth provide pinpoint military accuracy, see how bad guys can manipulate Google to create super worms, and see how they can "mash up" Google with Facebook, LinkedIn, and more for passive reconnaissance. This third edition includes completely updated content throughout and all new hacks such as Google scripting and using Google hacking with other search engines and APIs. Noted author Johnny Long, founder of Hackers for Charity, gives you all the tools you need to conduct the ultimate open source reconnaissance and penetration testing.

Authors: Johnny Long and Bill Gardner
Paperback: 234 pages
Publisher: Syngress; 3rd Revised edition (2015)
Language: English
ISBN-10: 0128029641

Wi-Foo: The Secrets of Wireless Hacking - most white papers and books available on wireless security are centered around 802.11 standards. Most explain the built-in security features of 802.11 protocols, explain future security standards development and requirements, list (and sometimes describe in detail) known security weaknesses of 802.11 networks, and describe the countermeasures that a wireless network manager or system administrator can take to reduce the risks presented by these flaws. Wireless networks are quickly becoming commonplace rather than the luxury that they were only two years ago. Wireless networks are everywhere from college dorms to developing nations and corporate settings.

As the wireless network becomes more pervasive additional technologies and standards have been developed to support them. Many current telecommunications and wireless networking books are undergoing revision to cover WiMax, ZigBee, 802.15, 802.16, and recent developments in Bluetooth. Keeping up to date with the contemporary list of threats, as well as the devices and standards to defend against them is vital to organizations and their networks. Wi Foo II: The Secrets of Wireless Hacking teaches penetration testers how to evaluate the security of a wireless network, and then show administrators how to fortify their networks, going beyond just 802.11. This newly updated and revised edition of the hit first edition will help administrators’ know of, prepare for, and defend against these threats.

Authors: Andrew Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky
Paperback: 624 pages
Publisher: Addison-Wesley Professional; 2nd edition (October 2007)
Language: English
ISBN-10: 0321393716
Hacking Exposed 7: Network Security Secrets and Solutions – bolster your system’s security and defeat the tools and tactics of cyber-criminals with expert advice and defense strategies from the world-renowned Hacking Exposed team. Case studies expose the hacker’s latest devious methods and illustrate field-tested remedies. Find out how to block infrastructure hacks, minimize advanced persistent threats, neutralize malicious code, secure web and database applications, and fortify UNIX networks. Hacking Exposed 7: Network Security Secrets & Solutions contains all-new visual maps and a comprehensive “countermeasures cookbook

Authors: Stuart McClure and Joel Scambray
Paperback: 768 pages
Publisher: McGraw-Hill Osborne; 7th edition (1 Aug. 2012)
Language: English
ISBN-10: 0071780289

Professional Pen Testing for Web Applications – there is no such thing as "perfect security" when it comes to keeping all systems intact and functioning properly. Good penetration (pen) testing creates a balance that allows a system to be secure while simultaneously being fully functional. With this book, you'll learn how to become an effective penetrator (i.e., a white hat or ethical hacker) in order to circumvent the security features of a Web application so that those features can be accurately evaluated and adequate security precautions can be put in place.

Author: Andres Andreu
Paperback: 522 pages
Publisher: Wrox; 1st edition (July 5, 2006)
Language: English
ISBN-10: 0471789666

Mastering Metasploit - the Metasploit framework has been around for a number of years and is one of the most widely used tools for carrying out penetration testing on various services. This book is a hands-on guide to penetration testing using Metasploit and covers its complete development. It will help you clearly understand the creation process of various exploits and modules and develop approaches to writing custom functionalities into the Metasploit framework.
This book covers a number of techniques and methodologies that will help you learn and master the Metasploit framework. You will also explore approaches to carrying out advanced penetration testing in highly secured environments, and the book’s hands-on approach will help you understand everything you need to know about Metasploit.

Author: Nipun Jaswal
Paperback: 378 pages
Publisher: Packt Publishing - ebooks Account (May 11, 2014)
Language: English
ISBN-10: 1782162224

**Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research** – This is the first book available for the Metasploit Framework (MSF), which is the attack platform of choice for one of the fastest growing careers in IT security: Penetration Testing. The book and companion Web site will provide professional penetration testers and security researchers with a fully integrated suite of tools for discovering, running, and testing exploit code.

This book discusses how to use the Metasploit Framework (MSF) as an exploitation platform. The book begins with a detailed discussion of the three MSF interfaces: msfweb, msfconsole, and msfcli. This chapter demonstrates all of the features offered by the MSF as an exploitation platform. With a solid understanding of MSF’s capabilities, the book then details techniques for dramatically reducing the amount of time required for developing functional exploits.

By working through real-world vulnerabilities against popular closed source applications, the reader will learn how to use the tools and MSF to quickly build reliable attacks as standalone exploits. The section will also explain how to integrate an exploit directly into the Metasploit Framework by providing a line-by-line analysis of an integrated exploit module. Details as to how the Metasploit engine drives the behind-the-scenes exploitation process will be covered, and along the way the reader will come to understand the advantages of exploitation frameworks. The final section of the book examines the Meterpreter payload system and teaches readers to develop completely new extensions that will integrate fluidly with the Metasploit Framework.

Author: James Foster
Paperback: 350 pages
Publisher: Syngress; 1 edition (October 2, 2007)
Language: English
ISBN-10: 1597490741
**Burp Suite Essentials** – if you are interested in learning how to test web applications and the web part of mobile applications using Burp, then this book by author Akash Mahajan is for you. It is specifically designed to meet your needs if you have basic experience in using Burp and are now aiming to become a professional Burp user.

Author: Akash Mahajan  
Paperback: 144 pages  
Publisher: Packt Publishing (28 Nov. 2014)  
Language: English  
ISBN-10: 1783550112  

**Instant Burp Suite Starter** – If you are an application developer with a focus on security then this practical guide by author Luca Carettoni is for you. Even with basic knowledge of security you will be able to develop your expertise and make your applications bulletproof.

Author: Luca Carettoni  
Paperback: 70 pages  
Publisher: Packt Publishing (25 Jan. 2013)  
Language: English  
ISBN-10: 1849695180  

**Basic Security Testing with Kali Linux** – with computer hacking attacks making headline news on a frequent occasion, it is time for companies and individuals to take a more active stance in securing their computer systems. Kali Linux by author Daniel W. Dieterle is an Ethical Hacking platform that allows good guys to use the same tools and techniques that a hacker would use so they can find issues with their security before the bad guys do.

In this book you will learn basic examples of how hackers find out information about your company, locate weaknesses in your security and how they gain access to your system.

Author: Daniel W. Dieterle  
Paperback: 312 pages  
Publisher: CreateSpace Independent Publishing Platform; 1st edition (5 Jan. 2014)  
Language: English  
ISBN-10: 1494861275  
Kali Linux Wireless Penetration Testing Essentials – this book is targeted at information security professionals, penetration testers and network/system administrators who want to get started with wireless penetration testing. No prior experience with Kali Linux and wireless penetration testing is required, but familiarity with Linux and basic networking concepts is recommended.

Author: Marco Alamanni
Paperback: 164 pages
Publisher: Packt Publishing (30 July 2015)
Language: English
ISBN-10: 1785280856

Kali Linux Network Scanning - will introduce you to critical scanning concepts. You will be shown techniques associated with a wide range of network scanning tasks that include discovery scanning, port scanning, service enumeration, operating system identification, vulnerability mapping, and validation of identified findings. You will learn how to utilize the arsenal of tools available in Kali Linux to conquer any network environment. You will also be shown how to identify remote services, how to assess security risks, and how various attacks are performed. This immersive guide will also encourage the creation of personally scripted tools and the development of skills required to create them.

Author: Justin Hutchens
Paperback: 400 pages
Publisher: Packt Publishing - ebooks Account (August 26, 2014)
Language: English
ISBN-10: 1783982144

Mastering Kali Linux for Advanced Penetration Testing - will teach you the kill chain perspective in assessing network security—from selecting the most effective tools, to rapidly compromising network security, to highlighting the techniques used to avoid detection. This book will take you, as a tester, through the reconnaissance, exploitation, and post-exploitation activities used by penetration testers and hackers.

After learning the hands-on techniques to perform an effective and covert attack, specific routes to the target will be examined, including bypassing physical security. You will also get to grips with concepts such as social engineering, attacking wireless networks, web services, and remote access connections. Finally, you will focus on the most vulnerable part of the network—directly attacking the end user. This book will provide all the practical knowledge
needed to test your network's security using a proven hacker's methodology.

Author: Robert W. Beggs  
Paperback: 325 pages  
Publisher: Packt Publishing - ebooks Account (May 21, 2014)  
Language: English  
ISBN-10: 1782163123  

**Ethical Hacking and Penetration, Step by Step with Kali Linux** - this book is a complete guide for those who would like to become an Ethical hacker. In this book you will learn what the Ethical hacking and its procedure is. The first couple of chapters are the definitions, concepts and process of becoming an Ethical hacker while the next half of the book will show in detail how to use certain tools and techniques to initiate attacks and penetrate a system. After reading this book, you should be able to use these tools to do some testing and even working on penetration projects. You just need to remember not to use these techniques in a production environment without having a formal approval.

Author: Rassoul Ghaznavi-zadeh  
Publisher: Primedia E-launch LLC (November 23, 2014)  
Publication Date: November 23, 2014  
Sold by: Amazon Digital Services, Inc.  
Language: English  
ASIN: B00Q3EWU6E

**Kali Linux: Assuring Security By Penetration Testing** - is a fully focused, structured book providing guidance on developing practical penetration testing skills by demonstrating cutting-edge hacker tools and techniques with a coherent, step-by-step approach. This book offers you all of the essential lab preparation and testing procedures that reflect real-world attack scenarios from a business perspective, in today's digital age.

Authors: Tedi Heriyanto, Lee Allen, Shakeel Ali  
Paperback: 454 pages  
Publisher: Packt Publishing - ebooks Account (May 9, 2014)  
Language: English  
ISBN-10: 184951948X  

**Penetration Testing** – in this book security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pen tester needs. Using a virtual machine-based lab that includes Kali Linux and vulnerable operating systems, you'll run
through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you’ll experience the key stages of an actual assessment - including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more.

Author: Georgia Weidman
Paperback: 528 pages
Publisher: No Starch Press; 1 edition (June 8, 2014)
Language: English
ISBN-10: 1593275641

The Mobile Application Hacker's Handbook – is a comprehensive guide to securing all mobile applications by approaching the issue from a hacker's point of view. Heavily practical, this book provides expert guidance toward discovering and exploiting flaws in mobile applications on the iOS, Android, Blackberry, and Windows Phone platforms. You will learn a proven methodology for approaching mobile application assessments, and the techniques used to prevent, disrupt, and remediate the various types of attacks. Coverage includes data storage, cryptography, transport layers, data leakage, injection attacks, runtime manipulation, security controls, and cross–platform apps, with vulnerabilities highlighted and detailed information on the methods hackers use to get around standard security.

Authors: Dominic Chell, Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse
Paperback: 816 pages
Publisher: John Wiley & Sons; 1 edition (3 April 2015)
Language: English
ISBN-10: 1118958500

The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws – web applications are the front door to most organizations, exposing them to attacks that may disclose personal information, execute fraudulent transactions, or compromise ordinary users. This practical book has been completely updated and revised to discuss the latest step–by–step techniques for attacking and defending the range of ever–evolving web applications. You’ll explore the various new technologies employed in web applications that have appeared since the first edition and review the new attack techniques that have been developed, particularly in relation to the client side.
Hackers Playbook 2 – just as a professional athlete doesn’t show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans. Written by a long-time security professional and CEO of Secure Planet, LLC, this step-by-step guide to the “game” of penetration hacking features hands-on examples and helpful advice from the top of the field.

Through a series of football-style “plays,” this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing—including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From “Pregame” research to “The Drive” and “The Lateral Pass,” the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mind-set of a penetration tester of a Fortune 500 company, regardless of your career or level of experience.

Author: Peter Kim
Paperback: 358 pages
Publisher: CreateSpace Independent Publishing Platform (June 20, 2015)
Language: English
ISBN-10: 1512214566

Metasploit: The Penetration Tester’s Guide – The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester’s Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors.

Once you’ve built your foundation for penetration testing, you’ll learn the Framework’s conventions, interfaces, and module system as you launch simulated attacks. You’ll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks.

Authors: David Kennedy and Jim O’Gorman
Paperback: 328 pages
Publisher: No Starch Press; 1 edition (25 July 2011)
Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions – as recent breaches like Target and Neiman Marcus show, payment card information is involved in more security breaches than any other data type. In too many places, sensitive card data is simply not protected adequately.

*Hacking Point of Sale* is a compelling book that tackles this enormous problem head–on. Exploring all aspects of the problem in detail – from how attacks are structured to the structure of magnetic strips to point–to–point encryption, and more – it's packed with practical recommendations. This terrific resource goes beyond standard PCI compliance guides to offer real solutions on how to achieve better security at the point of sale.

Author: Slava Gomzin
Paperback: 312 pages
Publisher: John Wiley & Sons; 1 edition (25 Mar. 2014)
Language: English
ISBN-10: 1118810112

RTFM: Red Team Field Manual – The Red Team Field Manual (RTFM) is a no fluff, but thorough reference guide for serious Red Team members who routinely find themselves on a mission without Google or the time to scan through a man page. The RTFM contains the basic syntax for commonly used Linux and Windows command line tools, but it also encapsulates unique use cases for powerful tools such as Python and Windows PowerShell. The RTFM will repeatedly save you time looking up the hard to remember Windows nuances such as Windows wmic and dsquery command line tools, key registry values, scheduled tasks syntax, startup locations and Windows scripting. More importantly, it should teach you some new red team techniques.

Author: Ben Clark
Paperback: 96 pages
Publisher: CreateSpace Independent Publishing Platform; 1.0 edition (11 Feb. 2014)
Language: English
ISBN-10: 1494295504
The Android Hacker's Handbook – As the Android operating system continues to increase its share of the smartphone market, smartphone hacking remains a growing threat. Written by experts who rank among the world's foremost Android security researchers, this book presents vulnerability discovery, analysis, and exploitation tools for the good guys. Following a detailed explanation of how the Android OS works and its overall security architecture, the authors examine how vulnerabilities can be discovered and exploits developed for various system components, preparing you to defend against them.

Authors: Joshua J. Drake and Zach Lanier
Paperback: 576 pages
Publisher: John Wiley & Sons; 1 edition (18 April 2014)
Language: English
ISBN-10: 111860864X

Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers – this book shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker's tools, this book will teach you to forge your own weapons using the Python programming language. This book demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts. It also shows how to write code to intercept and analyze network traffic using Python, craft and spoof wireless frames to attack wireless and Bluetooth devices, and how to data-mine popular social media websites and evade modern anti-virus. This book is a must have for Pythonistas who want to venture into penetration testing, open source intelligence gathering, wireless auditing and forensic analysis.

Author: TJ O'Connor
Paperback: 276 pages
Publisher: Syngress (8 Nov. 2012)
Language: English
ISBN-10: 1597499579

Black Hat Python: Python Programming for Hackers and Pentesters – This book is written by Justin Seitz, a senior security researcher at Immunity Inc. and the author of Gray Hat Python. This book is ideal for intermediate programmers who want to create a Github-Adware Trojan, extending the Burp proxy with python, network sniffers, web fuzzers or scrapers, keyloggers, and other offensive python projects. When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security
analysts. But just how does the magic happen?

In *Black Hat Python*, the latest from Justin Seitz (author of the best-selling *Gray Hat Python*), you'll explore the darker side of Python's capabilities—writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy Trojans, and more.

Author: Justin Seitz  
Paperback: 192 pages  
Publisher: No Starch Press; 1 edition (14 Dec. 2014)  
Language: English  
ISBN-10: 1593275900  

**The Browser Hacker's Handbook** — this book is written by Wade Alcorn, Christian Frichot, and Michele Orru' and they are the developers of BeEF (Browser Exploitation Framework) Project. The book gives a practical understanding of hacking the everyday web browser and using it as a beachhead to launch further attacks deep into corporate networks. Written by a team of highly experienced computer security experts, the handbook provides hands-on tutorials exploring a range of current attack methods.

The web browser has become the most popular and widely used computer "program" in the world. As the gateway to the Internet, it is part of the storefront to any business that operates online, but it is also one of the most vulnerable entry points of any system. With attacks on the rise, companies are increasingly employing browser-hardening techniques to protect the unique vulnerabilities inherent in all currently used browsers.

Author: Wade Alcorn and Christian Frichot  
Paperback: 648 pages  
Publisher: John Wiley & Sons; 1 edition (8 April 2014)  
Language: English  
ISBN-10: 1118662091  

**Hacking: The Art of Exploitation, 2nd Edition** — Hacking is the art of creative problem solving, whether that means finding an unconventional solution to a difficult problem or exploiting holes in sloppy programming. Many people call themselves hackers, but few have the strong technical foundation needed to really push the envelope.

Rather than merely showing how to run existing exploits, author Jon Erickson explains how arcane hacking techniques actually work. To share the art and science of hacking in a way that is accessible to everyone, *Hacking: The Art of Exploitation, 2nd Edition* introduces the
fundamentals of C programming from a hacker's perspective. Readers should have a fair understanding of Assembly, C, C++ programming languages to enjoy this book.

Author: Jon Erickson
Paperback: 480 pages
Language: English
ISBN-10: 1593271441

A Bug Hunter’s Diary: A Guided Tour Through the Wilds of Software Security – this book is a story and proof-of-concepts on how Tobias Klein found bugs for applications like VideoLAN’s VLC media player, Sun Solaris kernel, FFmpeg multimedia library, WebEx ActiveX, Avast! AV, OSX TTY IOCTL, etc. by getting or gaining the control of the instruction or program counter control (EIP, RIP, R15 or PC). The book does not include a working exploit code or a shellcode since the author’s home country (Germany) forbids the distribution of hacking tools, scanners and exploits.

Author: Tobias Klein
Paperback: 208 pages
Publisher: No Starch Press; 1 edition (14 Nov. 2011)
Language: English
ISBN-10: 1593273851

Nmap Essentials - Nmap is an extremely powerful network port scanner used to identify hosts on a network. Nmap is free, flexible, powerful, and easy to implement, which makes it a very convenient utility. This book demonstrates how to run basic and advanced scans, optimizing them to perform well in a variety of environments. Starting with an overview of Nmap, the reader will be guided through installation on popular operating systems. The book then explains how to use Nmap to run basic and advanced scans in addition to using the Nmap Scripting Engine (NSE). All this helps with optimizing Nmap performance in a variety of environments, eventually enabling the reader to integrate with other Nmap tools such as Nessus, Nikto, Burp Suite, and NSE versus NASL scanning. By the end of the book, the reader will have gained essential insights into network security analysis.

Author: David Shaw
Paperback: 141 pages
Publisher: Packt Publishing - ebooks Account (May 27, 2015)
Language: English
ISBN-10: 1783554061
Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning – Nmap Network Scanning is the official guide to the Nmap Security Scanner, a free and open source utility used by millions of people for network discovery, administration, and security auditing.

From explaining port scanning basics for novices to detailing low-level packet crafting methods used by advanced hackers, this book suits all levels of security and networking professionals. A 42-page reference guide documents every Nmap feature and option, while the rest of the book demonstrates how to apply those features to quickly solve real-world tasks.

Author: Gordon Fyodor Lyon
Paperback: 464 pages
Publisher: Nmap Project (1 Jan. 2009)
Language: English
ISBN-10: 0979958717

Nmap 6 Cookbook: The Fat Free Guide to Network Security Scanning – the Nmap 6 Cookbook provides simplified coverage of network scanning features available in the Nmap suite of utilities. Every Nmap feature is covered with visual examples to help you quickly understand and identify proper usage for practical results.

Author: Nicholas Marsh
Paperback: 226 pages
Publisher: CreateSpace Independent Publishing Platform; 6th edition (February 1, 2015)
Language: English
ISBN-10: 1507781385

Applied Network Security Monitoring - is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach, complete with real-world examples that teach you the key concepts of NSM.

Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, your ability to detect and respond to that intrusion can be the difference between a small incident and a major disaster. The book follows the
three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical knowledge that you can apply immediately.

Author: Chris Sanders and Jason Smith
Paperback: 496 pages
Publisher: Syngress; 1 edition (December 19, 2013)
Language: English
ISBN-10: 0124172083

Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground – former hacker Kevin Poulsen has, over the past decade, built a reputation as one of the top investigative reporters on the cybercrime beat. In Kingpin, he pours his unmatched access and expertise into book form for the first time, delivering a gripping cat-and-mouse narrative—and an unprecedented view into the twenty-first century’s signature form of organized crime.

Author: Kevin Poulsen
Paperback: 288 pages
Publisher: Broadway Books; Reprint edition (February 7, 2012)
Language: English
ISBN-10: 0307588696

Gray Hat Hacking: The Ethical Hacker’s Handbook – fortify your network and avert digital catastrophe with proven strategies from a team of security experts. Completely updated and featuring 12 new chapters, Gray Hat Hacking: The Ethical Hacker’s Handbook, Fourth Edition explains the enemy’s current weapons, skills, and tactics and offers field-tested remedies, case studies, and ready-to-deploy testing labs. Find out how hackers gain access, overtake network devices, script and inject malicious code, and plunder Web applications and browsers. Android-based exploits, reverse engineering techniques, and cyber law are thoroughly covered in this state-of-the-art resource.

Authors: Daniel Regalado and Shon Harris
Paperback: 656 pages
Language: English
ISBN-10: 0071832386
Social Engineering: The Art of Human Hacking – the first book to reveal and dissect the technical aspect of many social engineering manoeuvres. From elicitation, pretexting, influence and manipulation all aspects of social engineering are picked apart, discussed and explained by using real world examples, personal experience and the science behind them to unravel the mystery in social engineering.

Kevin Mitnick — one of the most famous social engineers in the world—popularized the term “social engineering.” He explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system. Mitnick claims that this social engineering tactic was the single—most effective method in his arsenal. This indispensable book examines a variety of manoeuvres that are aimed at deceiving unsuspecting victims, while it also addresses ways to prevent social engineering threats.

Author: Kevin Mitnick
Paperback: 416 pages
Publisher: John Wiley & Sons; 1st edition (17 Dec. 2010)
Language: English
ISBN-10: 0470639539

Social Engineering in IT Security: Tools, Tactics and Techniques – Conduct ethical social engineering tests to identify an organization’s susceptibility to attack. Written by a global expert on the topic, Social Engineering in IT Security discusses the roots and rise of social engineering and presents a proven methodology for planning a test, performing reconnaissance, developing scenarios, implementing the test, and accurately reporting the results. Specific measures you can take to defend against weaknesses a social engineer may exploit are discussed in detail. This practical guide also addresses the impact of new and emerging technologies on future trends in social engineering.

Author: Sharon Conheady
Paperback: 272 pages
Publisher: McGraw-Hill Professional (1 Aug. 2014)
Language: English
ISBN-10: 0071818464

Reversing: Secrets of Reverse Engineering – Beginning with a basic primer on reverse engineering—including computer internals, operating systems, and assembly language—and then discussing the various applications of reverse engineering, this book provides readers with practical, in-depth techniques for software reverse engineering. The book is broken into
two parts, the first deals with security-related reverse engineering and the second explores the more practical aspects of reverse engineering. In addition, the author explains how to reverse engineer a third-party software library to improve interfacing and how to reverse engineer a competitor's software to build a better product.

Author: Eldad Eilam
Paperback: 624 pages
Publisher: Wiley; 1st edition (April 15, 2005)
Language: English
ISBN-10: 0764574817

Practical Reverse Engineering – analyzing how hacks are achieved, so as to stop them in the future. Reverse engineering is the process of analyzing hardware or software and understanding it, without having access to the source code or design documents. Hackers are able to reverse engineer systems and exploit what they find with scary results. Now the good guys can use the same tools to thwart these threats. Practical Reverse Engineering goes under the hood of reverse engineering for security analysts, security engineers, and system programmers, so they can learn how to use these same processes to stop hackers in their tracks.

Authors: Bruce Dang and Alexandre Gazet
Paperback: 384 pages
Publisher: John Wiley & Sons; 1 edition (11 April 2014)
Language: English
ISBN-10: 1118787315

Hacking Exposed Wireless: Wireless Security Secrets & Solutions – thoroughly updated to cover today's established and emerging wireless technologies, Hacking Exposed Wireless, second edition reveals how attackers use readily available and custom tools to target, infiltrate, and hijack vulnerable systems. This book discusses the latest developments in Wi-Fi, Bluetooth, ZigBee, and DECT hacking, and explains how to perform penetration tests, reinforce WPA protection schemes, mitigate packet injection risk, and lock down Bluetooth and RF devices. Cutting-edge techniques for exploiting Wi-Fi clients, WPA2, cordless phones, Bluetooth pairing, and ZigBee encryption are also covered in this fully revised guide.

Authors: Jonny Cache, Vincent Liu, Joshua Wright
Series: Hacking Exposed
Paperback: 484 pages
Publisher: McGraw-Hill Osborne Media; 2nd edition (July 9, 2010)

Hacking Exposed Wireless, Third Edition features expert coverage of ever-expanding threats that affect leading-edge technologies, including Bluetooth Low Energy, Software Defined Radio (SDR), ZigBee, and Z-Wave.

Authors: Joshua Wright, Jonny Cache
Series: Hacking Exposed
Paperback: 560 pages
Publisher: McGraw-Hill Education; 3rd edition (March 16, 2015)
Language: English
ISBN-10: 0071827633

Hacking Wireless Networks - The ultimate hands-on guide - is a book written for people who seek to practice the techniques of assessing the security of wireless infrastructures. Through 30 real life scenarios and more than 300 figures the book examines in details the following areas: - Discovery and Profiling of wireless networks - Denial of Service attacks - Attacks against WEP secured wireless networks - Attacks against WPA/WPA2 secured wireless networks - Bypass techniques for popular Authentication mechanisms - Encryption keys cracking using special techniques - Attacks against the Access Point's management interface - Attacks against special security features like WPS - Stealthy techniques to avoid getting caught by wireless IDS Now that the world agrees that wireless security is central to computer security, it is time to put theory into practice.

Author: Andreas Kolokithas
Paperback: 428 pages
Publisher: CreateSpace Independent Publishing Platform (March 5, 2015)
Language: English
ISBN-10: 1508476349
Ruby on Rails Tutorial (3rd Edition) – The Ruby on Rails Tutorial book and screencast series teach you how to develop and deploy real, industrial-strength web applications with Ruby on Rails, the open-source web framework that powers top websites such as Twitter, Hulu, GitHub, and the Yellow Pages. The Ruby on Rails Tutorial book is available for free online and is available for purchase as an e-book (PDF, EPUB, and MOBI formats). The companion screencast series includes 12 individual lessons, one for each chapter of the Ruby on Rails Tutorial book. All purchases also include a free copy of the Solutions Manual for Exercises, with solutions to every exercise in the book.

Authors: Michael Hartl and Aurelius Prochazka
Paperback: 744 pages
Publisher: Addison Wesley; 3 edition (29 April 2015)
Language: English
ISBN-10: 0134077709

Building Secure Software: How to Avoid Security Problems the Right Way - cuts to the heart of computer security to help you get security right the first time. If you are serious about computer security, you need to read this book, which includes essential lessons for both security professionals who have come to realize that software is the problem, and software developers who intend to make their code behave. Written for anyone involved in software development and use—from managers to coders—this book is your first step toward building more secure software.

Building Secure Software provides expert perspectives and techniques to help you ensure the security of essential software. If you consider threats and vulnerabilities early in the development cycle you can build security into your system. With this book you will learn how to determine an acceptable level of risk, develop security tests, and plug security holes before software is even shipped.
Authors: John Viega and Gary McGraw
Series: Addison-Wesley Professional Computing Series
Paperback: 528 pages
Publisher: Addison-Wesley Professional; 1 edition (October 4, 2001)
Language: English
ISBN-10: 0321774957
Software Security: Building Security In 1st Edition - Beginning where the best-selling book Building Secure Software left off, Software Security teaches you how to put software security into practice. The software security best practices, or touchpoints, described in this book have their basis in good software engineering and involve explicitly pondering security throughout the software development lifecycle. This means knowing and understanding common risks (including implementation bugs and architectural flaws), designing for security, and subjecting all software artifacts to thorough, objective risk analyses and testing.

Software Security is about putting the touchpoints to work for you. Because you can apply these touchpoints to the software artifacts you already produce as you develop software, you can adopt this book’s methods without radically changing the way you work.

Author: Gary McGraw
Paperback: 448 pages
Publisher: Addison-Wesley Professional; 1 edition (February 2, 2006)
Language: English
ISBN-10: 0321356705

Secure Software Development: A Security Programmer's Guide 1st Edition – learn the essentials of developing secure software in accordance with the most current industry standards, in this comprehensive instructional guide. Secure Software Development: A Programmer's Guide leads readers through the tasks and activities that successful computer programmers navigate on a daily basis, from reading and analyzing requirements to choosing development tools, to guarding against software vulnerabilities and attacks. Additional coverage includes coding with built-in quality and security measures, and follow-up testing once a project is completed. With clear, straightforward examples and actual code snippets, readers can feel confident that they will gain the skills needed to develop software with all the critical components that ensure quality and security.

Authors: Jason Grembi
Paperback: 336 pages
Publisher: Delmar Cengage Learning; 1 edition (May 8, 2008)
Language: English
ISBN-10: 1418065471
**Writing Secure Code (2nd Edition) (Developer Best Practices)** – keep black-hat hackers at bay with the tips and techniques in this entertaining, eye-opening book! Developers will learn how to padlock their applications throughout the entire development process—from designing secure applications to writing robust code that can withstand repeated attacks to testing applications for security flaws. Easily digested chapters reveal proven principles, strategies, and coding techniques.

The authors—two battle-scarred veterans who have solved some of the industry’s toughest security problems—provide sample code in several languages. This edition includes updated information about threat modeling, designing a security process, international issues, file-system issues, adding privacy to applications, and performing security code reviews. It also includes enhanced coverage of buffer overruns, Microsoft .NET security, and Microsoft ActiveX development, plus practical checklists for developers, testers, and program managers.

*Author: David LeBlanc  and Michael Howard
Series: Developer Best Practices
Paperback: 800 pages
Publisher: Microsoft Press; 2nd edition (December 14, 2002)
Language: English
ISBN-10: 0735617228

**Exploiting Software: How to Break Code 1st Edition** – How does software break? How do attackers make software break on purpose? Why are firewalls, intrusion detection systems, and antivirus software not keeping out the bad guys? What tools can be used to break software? This book provides the answers.

*Exploiting Software* is loaded with examples of real attacks, attack patterns, tools, and techniques used by bad guys to break software. If you want to protect your software from attack, you must first learn how real attacks are really carried out. This must-have book may shock you—and it will certainly educate you.

*Authors: Gary McGraw and Greg Hoglund
Paperback: 512 pages
Publisher: Addison-Wesley Professional; 1st edition (February 27, 2004)
Language: English
ISBN-10: 0201786958
The Code Book: How to Make It, Break It, Hack It, Crack It — it’s known as the science of secrecy. Cryptography: the encoding and decoding of private information. And it is history’s most fascinating story of intrigue and cunning. From Julius Caesar and his Caesar Cipher to the code used by Mary Queen of Scots and her conspiracy to the use of the Enigma machine during the Second World War, Simon Singh follows the evolution of secret writing.

Accessible, compelling, and timely, this international bestseller, now adapted for young people (from 12-years up), is sure to make readers see the past—and the future—in a whole new way.

Author: Simon Singh
Hardcover: 272 pages
Publisher: Delacorte Books for Young Readers; 1st edition (March 12, 2002)
Language: English
ISBN-10: 0385729138

Cryptography Engineering — is written by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, a team of world-renowned cryptography experts. This essential guide is the definitive introduction to all major areas of cryptography: message security, key negotiation, and key management. You’ll learn how to think like a cryptographer. You’ll discover techniques for building cryptography into products from the start and you’ll examine the many technical changes in the field.

Authors: Niels Ferguson and Bruce Schneier
Paperback: 384 pages
Publisher: Wiley; 1st edition (26 Feb. 2010)
Language: English
ISBN-10: 0470474246

Everyday Cryptography — is a self-contained and widely accessible introductory text. Almost no prior knowledge of mathematics is required since the book deliberately avoids the details of the mathematical techniques underpinning cryptographic mechanisms, though a short appendix is included for those looking for a deeper appreciation of some of the concepts involved.

By the end of this book, the reader will not only be able to understand the practical issues concerned with the deployment of cryptographic mechanisms, including the management of cryptographic keys, but will also be able to interpret future developments in this fascinating and increasingly important area of technology.
Cryptography: A very short introduction – this book is a clear and informative introduction to cryptography and data protection—subjects of considerable social and political importance. It explains what algorithms do, how they are used, the risks associated with using them, and why governments should be concerned. Important areas are highlighted, such as Stream Ciphers, block ciphers, public key algorithms, digital signatures, and applications such as e-commerce.

This book highlights the explosive impact of cryptography on modern society, with, for example, the evolution of the internet and the introduction of more sophisticated banking methods.

Secrets and Lies – bestselling author Bruce Schneier offers his expert guidance on achieving security on a network. Internationally recognized computer security expert Bruce Schneier offers a practical, straightforward guide to achieving security throughout computer networks. Schneier uses his extensive field experience with his own clients to dispel the myths that often mislead IT managers as they try to build secure systems. This practical guide provides readers with a better understanding of why protecting information is harder in the digital world, what they need to know to protect digital information, how to assess business and corporate security needs, and much more.
Beyond Fear – many of us, especially since 9/11, have become personally concerned about issues of security, and this is no surprise. Security is near the top of government and corporate agendas around the globe. Security-related stories appear on the front page every day. How well though, do any of us truly understand what achieving real security involves?

In Beyond Fear, Bruce Schneier invites us to take a critical look at not just the threats to our security, but the ways in which we’re encouraged to think about security by law enforcement agencies, businesses of all shapes and sizes, and our national governments and militaries. Schneier believes we all can and should be better security consumers, and that the trade-offs we make in the name of security - in terms of cash outlays, taxes, inconvenience, and diminished freedoms - should be part of an ongoing negotiation in our personal, professional, and civic lives, and the subject of an open and informed national discussion.

Author: Bruce Schneier
Hardcover: 308 pages
Language: English
ISBN-10: 0387026207

Internet Forensics – This practical guide to defending against Internet fraud gives you the skills you need to uncover the origins of the spammers, con artists, and identity thieves that plague the Internet. Targeted primarily at the developer community, Internet Forensics shows you how to extract the information that lies hidden in every email message, web page, and web server on the Internet. It describes the lengths the bad guys will go to cover their tracks, and offers tricks that you can use to see through their disguises. You'll also gain an understanding for how the Internet functions, and how spammers use these protocols to their devious advantage.

The book is organized around the core technologies of the Internet-email, web sites, servers, and browsers. Chapters describe how these are used and abused and show you how information hidden in each of them can be revealed. Short examples illustrate all the major techniques that are discussed. The ethical and legal issues that arise in the uncovering of Internet abuse are also addressed.

Not surprisingly, the audience for Internet Forensics is boundless. For developers, it's a serious foray into the world of Internet security; for weekend surfers fed up with spam, it's an entertaining and fun guide that lets them play amateur detective from the safe confines of their home or office.
Windows Forensics Analysis Toolkit: W8 Edition - The primary focus of this edition is on analyzing Windows 8 systems and processes using free and open-source tools. The book covers live response, file analysis, malware detection, timeline, and much more. Harlan Carvey presents real-life experiences from the trenches, making the material realistic and showing the why behind the how.

The companion and toolkit materials are hosted online. This material consists of electronic printable checklists, cheat sheets, free custom tools, and walk-through demos. This edition complements Windows Forensic Analysis Toolkit, Second Edition, which focuses primarily on XP, and Windows Forensic Analysis Toolkit, Third Edition, which focuses primarily on Windows 7.

This new fourth edition provides expanded coverage of many topics beyond Windows 8 as well, including new cradle-to-grave case examples, USB device analysis, hacking and intrusion cases, and "how would I do this" from Harlan's personal case files and questions he has received from readers. The fourth edition also includes an all-new chapter on reporting.

Real Digital Forensics: Computer Security and Incident Response – In this book, a team of world-class computer forensics experts walks you through six detailed, highly realistic investigations and provides a DVD with all the data you need to follow along and practice. From binary memory dumps to log files, this DVD's intrusion data was generated by attacking live systems using the same tools and methods real-world attackers use. The evidence was then captured and analyzed using the same tools the authors employ in their own investigations.

This book relies heavily on open source tools, so you can perform virtually every task without investing in any commercial software. You'll investigate environments ranging from financial
institutions to software companies and crimes ranging from intellectual property theft to SEC violations. As you move step by step through each investigation, you'll discover practical techniques for overcoming the challenges forensics professionals face most often.

Authors: Keith Jones, Richard Bejtlich, Curtis Rose
Paperback: 688 pages
Publisher: Addison-Wesley Professional (October 3, 2005)
Language: English
ISBN-10: 9780321240699

**Measuring and Managing Information Risk: A FAIR Approach** – the authors have written a book that will change the way you think about and deal with IT risk. FAIR takes the FUD out of risk management, and provides a formal language to deal with risk.

Using the factor analysis of information risk (FAIR) methodology developed over ten years and adopted by corporations worldwide, Measuring and Managing Information Risk provides a proven and credible framework for understanding, measuring, and analyzing information risk of any size or complexity. Intended for organizations that need to either build a risk management program from the ground up or strengthen an existing one, this book provides a unique and fresh perspective on how to do a basic quantitative risk analysis. Covering such key areas as risk theory, risk calculation, scenario modeling, and communicating risk within the organization, Measuring and Managing Information Risk helps managers make better business decisions by understanding their organizational risk.

Authors: Dr. Jack Freund and Jack Jones
Paperback: 410 pages
Publisher: Butterworth-Heinemann (22 Aug. 2014)
Language: English
ISBN-10: 0124202314

**Security Metrics** - is the first comprehensive best-practice guide to defining, creating, and utilizing security metrics in the enterprise. Using sample charts, graphics, case studies, and war stories, Yankee Group Security Expert Andrew Jaquith demonstrates exactly how to establish effective metrics based on your organization's unique requirements. You'll discover how to quantify hard-to-measure security activities, compile and analyze all relevant data, identify strengths and weaknesses, set cost-effective priorities for improvement, and craft compelling messages for senior management.
Security Metrics successfully bridges management's quantitative viewpoint with the nuts-and-bolts approach typically taken by security professionals. It brings together expert solutions drawn from Jaquith’s extensive consulting work in the software, aerospace, and financial services industries, including new metrics presented nowhere else.

Author: Andrew Jaquith
Paperback: 336 pages
Publisher: Addison-Wesley Professional; 1st edition (April 5, 2007)
Language: English
ISBN-10: 0321349989

Threat Modeling: Designing for Security – Adam Shostack is responsible for security development lifecycle threat modeling at Microsoft and is one of a handful of threat modeling experts in the world. Now, he is sharing his considerable expertise into this unique book. With pages of specific actionable advice, he details how to build better security into the design of systems, software, or services from the outset. You'll explore various threat modeling approaches, find out how to test your designs against threats, and learn effective ways to address threats that have been validated at Microsoft and other top companies.

Author: Adam Shostack
Paperback: 624 pages
Publisher: John Wiley & Sons; 1st edition (25 April 2014)
Language: English
ISBN-10: 1118809998

Data-Driven Security: Analysis, Visualization and Dashboards – authors Jay Jacobs and Bob Rudis should be known as the security bad data busters. Rather than using FUD, they use empirical evidence. Read the book and uncover hidden patterns of data and respond with countermeasures. Security professionals need all the tools at their disposal to increase their visibility in order to prevent security breaches and attacks.

This careful guide explores two of the most powerful data analysis and visualization. You'll soon understand how to harness and wield data, from collection and storage to management and analysis as well as visualization and presentation. Using a hands-on approach with real-
world examples, this book shows you how to gather feedback, measure the effectiveness of your security methods, and make better decisions. Everything in this book will have practical application for information security professionals.

Authors: Jay Jacobs and Bob Rudis
Paperback
Publisher: Wiley (8 April 2014)
Language: English
ISBN-10: 1118793722

Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World – data is everywhere. We create it every time we go online, turn our phone on (or off!), or pay with a credit card. This data is stored, studied, and bought and sold by corporations and governments for surveillance and for control. Foremost security expert (Wired) and best-selling author Bruce Schneier shows how this data has led to a double-edged Internet a Web that gives power to the people but is abused by the institutions on which those people depend.

In Data and Goliath, Schneier reveals the full extent of surveillance, censorship, and propaganda in society today, examining the risks of cybercrime, cyberterrorism, and cyberwar. He shares technological, legal, and social solutions that can help shape a more equal, private, and secure world. This is a book everyone with an Internet connection or bank account, or smart device, or car, for that matter needs to read.

Author: Bruce Schneier
Hardcover: 400 pages
Publisher: W. W. Norton & Company (18 April 2015)
Language: English
ISBN-10: 0393244814

Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan – any good attacker will tell you that expensive security monitoring and prevention tools aren’t enough to keep you secure. This practical book demonstrates a data-centric approach to distilling complex security monitoring, incident response, and threat analysis ideas into their most basic elements. You’ll learn how to develop your own threat intelligence and incident detection strategy, rather than depend on security tools alone.

Written by members of Cisco’s Computer Security Incident Response Team, this book shows IT and information security professionals how to create an InfoSec playbook by developing
strategy, technique, and architecture.

Authors: Jeff Bollinger and Brandon Enright
Paperback: 276 pages
Publisher: O'Reilly Media; 1 edition (24 May 2015)
Language: English
ISBN-10: 1491949406

Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder – is a zero fluff reference guide for cyber security incident responders and InfoSec pros alike. The BTHb includes essential information in a condensed handbook format about the incident response process, how attackers work, common tools, a methodology for network analysis developed over 12 years, Windows and Linux analysis processes, tcpdump usage examples, Snort IDS usage, and numerous other topics.

The book is peppered with practical real life techniques from the authors extensive career working in academia and a corporate setting. Whether you are writing up your cases notes, analyzing potentially suspicious traffic, or called in to look over a misbehaving server – this book should help you handle the case and teach you some new techniques along the way.

Author: Don Murdoch
Paperback: 154 pages
Publisher: CreateSpace Independent Publishing Platform; 2nd edition (August 3, 2014)
Language: English
ISBN-10: 1500734756

The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (SEI Series in Software Engineering) 1st Edition - since 2001, the CERT® Insider Threat Center at Carnegie Mellon University’s Software Engineering Institute (SEI) has collected and analyzed information about more than seven hundred insider cyber crimes, ranging from national security espionage to theft of trade secrets. The CERT® Guide to Insider Threats describes CERT’s findings in practical terms, offering specific guidance and countermeasures that can be immediately applied by executives, managers, security officers, and operational staff within any private, government, or military organization.

The authors systematically address attacks by all types of malicious insiders, including
current and former employees, contractors, business partners, outsourcers, and even cloudcomputing vendors. They cover all major types of insider cyber crime: IT sabotage, intellectual property theft, and fraud. For each, they present a crime profile describing how the crime tends to evolve over time, as well as motivations, attack methods, organizational issues, and precursor warnings that could have helped the organization prevent the incident or detect it earlier. Beyond identifying crucial patterns of suspicious behavior, the authors present concrete defensive measures for protecting both systems and data.

This book also conveys the big picture of the insider threat problem over time: the complex interactions and unintended consequences of existing policies, practices, technology, insider mind-sets, and organizational culture. Most important, it offers actionable recommendations for the entire organization, from executive management and board members to IT, data owners, HR, and legal departments.

Authors: Dawn M. Cappelli, Andrew P. Moore, Randall F. Trzeciak
Series: SEI Series in Software Engineering
Hardcover: 432 pages
Publisher: Addison-Wesley Professional; 1 edition (February 3, 2012)
Language: English
ISBN-10: 0321812573

Security Operations Center: Building, Operating, and Maintaining your SOC – is the complete guide to building, operating, and managing Security Operations Centers in any environment. Drawing on experience with hundreds of customers ranging from Fortune 500 enterprises to large military organizations, three leading experts thoroughly review each SOC model, including virtual SOCs. You’ll learn how to select the right strategic option for your organization, and then plan and execute the strategy you’ve chosen.

This book walks you through every phase required to establish and run an effective SOC, including all significant people, process, and technology capabilities. The authors assess SOC technologies, strategy, infrastructure, governance, planning, implementation, and more. They take a holistic approach considering various commercial and open-source tools found in modern SOCs.

Author: Joseph Muniz and Gary McIntyre
Paperback: 448 pages
Publisher: Cisco Press; 1 edition (29 Oct. 2015)
Language: English
ISBN-10: 0134052013
Designing and Building a SOC – written by a subject expert who has consulted on SOC implementation in both the public and private sector, *Designing and Building a Security Operations Center* is the go-to blueprint for cyber-defense. If you’re committed to defending your own assets and your customers’ information this book will show you how to develop the organization, infrastructure, and capabilities to protect your company and your customers effectively, efficiently, and discreetly.

**Author:** David Nathans  
**Paperback:** 276 pages  
**Publisher:** Syngress; 1 edition (November 20, 2014)  
**Language:** English  
**ISBN-10:** 0128008997  
**ISBN-13:** 978-0128008997

The Tangled Web: A Guide to Securing Modern Web Applications – This book is written by Michal Zalewski a.k.a lcamtuf who is a one of the 15 most influential people in security, among the 100 most influential people in IT, and a security engineer from Google. In it he offers a compelling narrative that explains exactly how browsers work and why they’re fundamentally insecure.

Rather than dispense simplistic advice on vulnerabilities, Zalewski examines the entire browser security model, revealing weak points and providing crucial information for shoring up web application security. This is a must read for web developers and web security enthusiasts because it covers brief history of the web, browser security model, web application security, and has a section called Security Engineering Cheat Sheet.

**Author:** Michal Zalewski  
**Paperback:** 320 pages  
**Publisher:** No Starch Press; 1 edition (29 Nov. 2011)  
**Language:** English  
**ISBN-10:** 1593273886  
**ISBN-13:** 978-1593273880

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, this book will teach you the tools and techniques used by professional analysts. With this book as your guide, you’ll be able to safely analyze, debug, and disassemble any malicious software that comes your way.

**Author:**  
**Paperback:**  
**Publisher:**  
**Language:**  
**ISBN-10:**  
**ISBN-13:**

---

**Cyber Security Capital**
Malware, Rootkits & Botnets: A Beginner’s Guide – This book is written by Christopher C. Elisan who is the Principal Malware Scientist and Senior Manager of the Malware Intelligence Team at RSA, The Security Division of EMC. Learn how to improve the security posture of your organization and defend against some of the most pervasive network attacks. Malware, Rootkits & Botnets: A Beginner’s Guide explains the nature, sophistication, and danger of these risks and offers best practices for thwarting them.

After reviewing the current threat landscape, the book describes the entire threat lifecycle, explaining how cybercriminals create, deploy, and manage the malware, rootkits, and botnets under their control. You’ll learn proven techniques for identifying and mitigating these malicious attacks. Templates, checklists, and examples give you the hands-on help you need to get started protecting your network right away. The book is well written, organized and can easily be understood by newbies.

There Will Be Cyberwar: How The Move To Network-Centric War Fighting Has Set The Stage For Cyberwar – the move on the part of the US military, which began in 1996, to Network-Centric Warfare (NCW), meant the combination of sensor grids, C&C grids, and precision targeting to increase speed to command, and represented a military offset. Along with networking comes exposure to cyber attacks, attacks that will be used in future wars.

Author: Richard Stiennon
Paperback: 174 pages
Publisher: IT-Harvest Press (23 Mar. 2015)
Language: English
ISBN-10: 0985460784
Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon -
top cybersecurity journalist Kim Zetter tells the story behind the virus that sabotaged Iran’s nuclear efforts and shows how its existence has ushered in a new age of warfare—one in which a digital attack can have the same destructive capability as a megaton bomb.

Author: Kim Zetter
Paperback: 448 pages
Publisher: Broadway Books (September 1, 2015)
Language: English
ISBN-10: 0770436196

No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State – in May 2013, Glenn Greenwald set out for Hong Kong to meet an anonymous source who claimed to have astonishing evidence of pervasive government spying and insisted on communicating only through heavily encrypted channels. That source turned out to be the twenty-nine-year-old NSA contractor Edward Snowden, and his revelations about the agency’s widespread, systemic overreach proved to be some of the most explosive and consequential news in recent history, triggering a fierce debate over national security and information privacy.

Now Greenwald fits all the pieces together, recounting his high-intensity eleven-day trip to Hong Kong, examining the broader implications of the surveillance detailed in his reporting for The Guardian, and revealing fresh information on the NSA’s unprecedented abuse of power with documents from the Snowden archive. Fearless and incisive, No Place to Hide has already sparked outrage around the globe and been hailed by voices across the political spectrum as an essential contribution to our understanding of the U.S. surveillance state.

Author: Glenn Greenwald
Paperback: 304 pages
Publisher: Picador; Reprint edition (April 28, 2015)
Language: English
ISBN-10: 1250062586
Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists – this book provides a practical and comprehensive approach to information security and privacy law for both international and domestic statutes. It provides all the tools needed to handle the business, legal and technical risks of protecting information on a global scale. For anyone responsible for or advising a corporation involved in domestic or international business, who must comply with a dizzying array of statutes, regulations, technologies, methodologies and standards, this book is for you.

Authors: Thomas J Shaw
Paperback: 395 pages
Publisher: American Bar Association (February 16, 2012)
Language: English
ISBN-10: 161632807X

Navigating the Digital Age – is the definitive cybersecurity guide for boardroom members and executive officers. Developed in collaboration with the New York Stock Exchange Group and Palo Alto Networks, this one-of-a-kind anthology provides practical, actionable and expert advice on best practices for compliance, implementation, breach prevention and immediate response tactics for your company.

More info at: http://connect.paloaltonetworks.com/cyberhandbook

The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage (Novel) - Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter" -- a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information.

Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases -- a one-man sting operation that finally gained the attention of the CIA...and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

Author: Cliff Stoll
Paperback: 399 pages
Publisher: Pocket Books (September 13, 2005)
Language: English
ISBN-10: 1416507787
The Phoenix Project (Novel) – in a fast-paced and entertaining style, three luminaries of the DevOps movement deliver a story that anyone who works in IT will recognize. Readers will not only learn how to improve their own IT organizations; they’ll never view IT the same way again.

Authors: Kevin, Behr, George Spafford, Gene Kim
Paperback: 376 pages
Publisher: IT Revolution Press; Reprint edition (October 16, 2014)
Language: English
ISBN-10: 0988262509

Little Brother (Novel) - Marcus, a.k.a "w1n5t0n," is only seventeen years old, but he figures he already knows how the system works—how to work the system. Smart, fast, and wise to the ways of the networked world, he has no trouble outwitting his high school's intrusive but clumsy surveillance systems.

But his whole world changes when he and his friends find themselves caught in the aftermath of a major terrorist attack on San Francisco. In the wrong place at the wrong time, Marcus and his crew are apprehended by the Department of Homeland Security and whisked away to a secret prison where they're mercilessly interrogated for days.

When the DHS finally releases them, Marcus discovers that his city has become a police state where every citizen is treated like a potential terrorist. He knows that no one will believe his story, which leaves him only one option: to take down the DHS himself.

Author: Cody Doctorow
Paperback: 432 pages
Publisher: Tor Teen; 1 edition (April 13, 2010)
Language: English
ISBN-10: 0765323117
WHAT NEXT?

MY GOAL IS TO CONNECT, TRAIN AND MOBILISE A DIVERSE GLOBAL CYBER SECURITY WORKFORCE.

I want to see a more diverse range of professionals within the whole cyber security ecosystem and reduce the current skills shortage. I want more of you thrive and solve meaningful problems within the industry. I believe passionately in a diverse workplace and in safeguarding businesses, world economies, people and countries. Cyber security is a varied profession and there’s a huge need right now for all manners of cyber security expertise. I want to be part of a movement that develops this talent and fosters growth regardless of gender-biased discrimination.

By 2017, through Cyber Security Capital, I aim to have helped 1000 professionals live up to their full potential. I plan to do this by focusing on several initiatives, including the women in security book and gender diversity conference, and by providing the best mentoring, training and employment opportunities available to you globally.

I believe that as a professional who’s interested in cyber security you’ve much value to offer. If you’ve signed up and read this report, clearly you’re open to finding more ways to improve your opportunities as a cyber security professional. Starting in 2016 I’ll be running a series of global events for students, professionals, leaders and entrepreneurs within cyber security. I’ll also be working with small, select, groups of people in training programmes.

THE NEXT STEP IS TO REGISTER FOR OUR CYBER SECURITY GENDER DIVERSITY EVENT. YOU CAN FIND OUT MORE AT: bit.ly/22qWM70

FINALLY...

Thank you for reading this resource guide and taking a valuable step towards becoming a leading cyber security professional. Whilst there are always challenges to overcome as a cyber security professional, make no mistake there are more advantages available. And, whether you chose to become one now or not, or advance your skills within our industry is up to you. Cyber security isn’t for everyone. However, if it is and you’re intent on developing a successful career within it, it can bring unfold returns.
About the Author

Jane Frankland is a successful cyber security entrepreneur, author, speaker and business consultant. She is also a Board Advisor for ClubCISO, a nominated Cyber Security Woman of the Year 2016 and an SC Magazine Awards Judge. She has built and sold her own seven-figure cyber security consultancy and is frequently invited to speak about entrepreneurship, women in business and cyber security at events around the world.

She has over 18 years worth of experience in cyber security and has held directorships and senior executive positions within her own companies and at several large PLCs. Through her latest venture, Cyber Security Capital, she is now helping to connect, train and mobilise a cyber security workforce by providing innovative consulting and resourcing solutions.

Jane believes passionately in entrepreneurship, empowerment and freedom. Through her work she wants to help more individuals entre cyber security and develop to the best of their abilities. Furthermore, to see more businesses survive and thrive, free from cybercrime. She is particularly interested in diversity in the cyber security workplace and is currently creating a series of global events to showcase this along with a platform that will connect professionals from the whole cyber security ecosystem to mentors, training programmes, internships and employment.

Jane has a BA (Hons) from Loughborough University in Woven Textile Design, was a Nominated Young British Designer and is a Fellow of the Institute of Sales & Marketing (ISMM). She’s also a mother to three children, has a Weimaraner dog, a black and white moggy and several chickens. The question you’ll hear her ask the most in business is ‘what’s your objective?’ The reason why is obvious. Time is precious and unless you know why you’re doing something why do it at all.

Jane can be contacted on:

Email: hello@jane-frankland.com  
Twitter: https://twitter.com/JaneFrankland  
LinkedIn: https://linkedin.com/in/JaneFrankland