Iot Hacking Sicherheitslucken Im Internet Der Din

Getting the books **Iot Hacking Sicherheitslucken Im Internet Der Din** now is not type of challenging means. You could not only going gone book collection or library or borrowing from your links to read them. This is an unconditionally easy means to specifically acquire lead by on-line. This online statement Iot Hacking Sicherheitslucken Im Internet Der Din can be one of the options to accompany you in the manner of having extra time.

It will not waste your time. tolerate me, the e-book will enormously song you further matter to read. Just invest tiny mature to approach this on-line message **Iot Hacking Sicherheitslucken Im Internet Der Din** as skillfully as evaluation them wherever you are now.

Der Cyber Survival Guide - Nick Selby 2018-10-08
Identitätsdiebstahl. E-Mail-Hacks. Angriffe auf die Infrastruktur. Kreditkartenbetrug. Sogar Auftragsmord. All diese Verbrechen können mit nur wenigen Mausklicks begangen werden. Cyberkriminelle können Sie jederzeit angreifen: über den Laptop, das Smartphone, den Fernseher - sogar über Ihre Türklingel oder Ihr Thermostat. Die gute Nachricht? Sie müssen kein Opfer sein. In diesem umfassenden, praktischen und fundierten Handbuch geben Ihnen der Sicherheitsexperte Nick Selby und die Zukunftsforscherin Heather Vescent die nötigen Tools an die Hand, um Ihre Familie, Ihre Privatsphäre, Ihre Finanzen und Ihren Ruf zu schützen. Gehen Sie nicht ohne es online.
Hacking: The Next Generation - Nitesh Dhanjani 2009-08-29
With the advent of rich Internet applications, the explosion of social media, and the increased use of powerful cloud computing infrastructures, a new generation of attackers has added cunning new techniques to its arsenal. For anyone involved in defending an application or a network of systems, Hacking: The Next Generation is one of the few books to identify a variety of emerging attack vectors. You'll not only find valuable information on new hacks that attempt to exploit technical flaws, you'll also learn how attackers take advantage of individuals via social networking sites, and abuse vulnerabilities in wireless technologies and cloud infrastructures. Written by seasoned Internet security professionals, this book helps you understand the motives and psychology of hackers behind these attacks, enabling you to better prepare and defend against them. Learn how "inside out" techniques can poke holes into protected networks Understand the new wave of "blended threats" that take advantage of multiple application vulnerabilities to steal corporate data Recognize weaknesses in today's powerful cloud infrastructures and how they can be exploited Prevent attacks against the mobile workforce and their devices containing valuable data Be aware of attacks via social networking sites to obtain confidential information from executives and their assistants Get case studies that show how several layers of vulnerabilities can be used to compromise multinational corporations
Digital Privacy and Security Using Windows - Nihad Hassan 2017-07-02
Use this hands-on guide to understand the ever growing and complex world of digital security. Learn how to protect yourself from digital crime, secure your communications, and become anonymous online using sophisticated yet practical tools and techniques. This book teaches you how to secure your online identity and personal devices, encrypt your digital data and online communications, protect cloud data and Internet of Things (IoT), mitigate social engineering attacks, keep your purchases secret, and conceal your digital footprint. You will understand best practices to harden your operating system and delete digital traces using the most widely used operating system, Windows. Digital Privacy and Security Using Windows offers a comprehensive list of practical digital privacy tutorials in addition to being a complete repository of free online resources and tools assembled in one place. The book helps you build a robust defense from electronic crime and corporate surveillance. It covers general principles of digital privacy and how to configure and use various security applications to maintain your privacy, such as TOR, VPN, and BitLocker. You will learn to encrypt email communications using Gpg4win and Thunderbird. What You'll Learn Know the various parties interested in having your private data Differentiate between government and corporate surveillance, and the motivations behind each one Understand how online tracking works technically Protect digital data, secure online communications, and become anonymous online Cover and destroy your digital traces using Windows OS Secure your data in transit and at rest Be aware of cyber security risks and countermeasures Who This Book Is For End users, information security professionals, management, infosec students
Make: Special Internet der Dinge 2017 - Make-Redaktion 2016-11-28
Das Sonderheft des deutschsprachigen DIY-Magazins Make: zum Thema Internet der Dinge (Internet of Things - IoT) bietet einen leichten Einstieg. Die Praxisbeispiele zeigen, wie Sie verschiedene Geräte mit dem Internet verbinden und Daten weltweit empfangen und auswerten können oder wie sich aus der Ferne Module steuern lassen. In ausführlichen Grundlagenartikeln werden Sie mit den verschiedenen Funktechniken und Protokollen vertraut gemacht, erfahren wie mit DALI zu Hause das Licht kontrolliert wird und erproben am praktischen Beispiel MQTT und ZigBee mit Xbee. Mit Beacons können Sie kleine Leuchtfeuer setzen und so unter Anderem die Positionsbestimmung im Gebäuden optimieren. Die weiteren Beispiele erweitern Ihr Wissen und praktischen Fähigkeiten, in dem Sie sich eine eigene Amazon Echo mit einem Raspberry Pi nachbauen, Philips Hue-Lampen per Node-RED steuern, WLAN-Module mit Lua programmieren oder automatisch Familienfotos im digitalen Bilderrahmen mit Ihren Verwandten teilen.Die Redaktion der Zeitschrift Make: steht auch bei diesem Sonderheft für anspruchsvolle neue Artikel in der gewohnten übersichtlichen Aufmachung, die sicherstellt, dass die Projekte wie gezeigt nachvollzogen werden können und am Ende funktionieren. Learning by Doing steht bei Make: immer im Vordergrund.
Wireless Network Security - Yang Xiao 2007-12-29
This book identifies vulnerabilities in the physical layer, the MAC layer, the IP layer, the transport layer, and the application layer, of wireless networks, and discusses ways to strengthen security mechanisms and services. Topics covered include intrusion detection, secure PHY/MAC/routing protocols, attacks and prevention, immunization, key management, secure group communications and multicast, secure location services, monitoring and surveillance, anonymity, privacy, trust establishment/management, redundancy and security, and dependable wireless networking.
Wicked Cool Shell Scripts, 2nd Edition - Dave Taylor 2016-10-15
Shell scripts are an efficient way to interact with your machine and manage your files and system operations. With just a few lines of code, your computer will do exactly what you want it to do. But you can also use shell scripts for many other essential (and not-so-essential) tasks. This second edition of Wicked Cool Shell Scripts offers a collection of useful, customizable, and fun shell scripts for solving common problems and personalizing your computing environment. Each chapter contains ready-to-use scripts and explanations of how they work, why you'd want to use them, and suggestions for changing and expanding them. You'll find a mix of classic favorites, like a disk backup utility that keeps your files safe when your system crashes, a password manager, a weather tracker, and several games, as well as 23 brand-new scripts, including: – ZIP code lookup tool that reports the city and state – Bitcoin address information retriever – suite of tools for working with cloud services like Dropbox and iCloud – for renaming and applying commands to files in bulk – processing and editing tools Whether you want to save time managing your system or just find new ways to goof off, these scripts are wicked cool!
Cybersecurity Essentials - Charles J. Brooks 2018-08-31
An accessible introduction to cybersecurity concepts and practices Cybersecurity Essentials provides a comprehensive introduction to the field, with expert coverage of essential topics required for entry-level cybersecurity certifications. An effective defense consists of four distinct challenges: securing the infrastructure, securing devices, securing local networks, and securing the perimeter. Overcoming these challenges requires a detailed understanding of the concepts and practices within each realm. This book covers each challenge individually for greater depth of information, with real-world scenarios that show what vulnerabilities look like in everyday computing scenarios. Each part concludes with a summary of key concepts, review questions, and hands-on exercises, allowing you to test your understanding while exercising

your new critical skills. Cybersecurity jobs range from basic configuration to advanced systems analysis and defense assessment. This book provides the foundational information you need to understand the basics of the field, identify your place within it, and start down the security certification path. Learn security and surveillance fundamentals Secure and protect remote access and devices Understand network topologies, protocols, and strategies Identify threats and mount an effective defense Cybersecurity Essentials gives you the building blocks for an entry level security certification and provides a foundation of cybersecurity knowledge

Remaining Relevant - Rob Nixon 2015-03-27

'Remaining Relevant' is practical and practiced advice for accountants to remain relevant in a 'disrupted' industry and has been described as "the most important business book that you will read this year." Anthony S Bongiorno, The Bongiorno Group. The explosion of cloud computing and its impact on the accounting industry is the impetus for 'Remaining Relevant', which is all about the future of the accounting profession - essential reading in this manual for an accountant's success.

"Technology is enabling and will demand the accounting profession to transform. From the changing the engagement and service mix within a firm, to fixed fee billing and off shoring ... everything is up for review. As long-term industry insider and visionary, Rob has the unique capability to help accountants focus on what is important through his direct, and at times confronting, analysis of the profession. A must read." Tim Reed, MYOB CEO "Rob Nixon is to accounting what Peter Drucker was to strategy: He creates new paradigms and fresh approaches to a discipline that would be headed for the doldrums without him." Alan Weiss, PhD, Author, Million Dollar Consulting Rhode Island, USA "The accounting game is changing forever. Any partner who doesn't acknowledge this is kidding themselves. The age of the dinosaur firm is coming to an end, and this book is a must for any accountant who wants to remain relevant in the 21st Century." Chris Hooper, CEO, Accodex Adelaide, Australia

Cybersecurity: The Beginner's Guide - Dr. Erdal Ozkaya 2019-05-27

Understand the nitty-gritty of Cybersecurity with ease Key FeaturesAlign your security knowledge with industry leading concepts and toolsAcquire required skills and certifications to survive the ever changing market needsLearn from industry experts to analyse, implement, and maintain a robust environmentBook Description It's not a secret that there is a huge talent gap in the cybersecurity industry. Everyone is talking about it including the prestigious Forbes Magazine, Tech Republic, CSO Online, DarkReading, and SC Magazine, among many others. Additionally, Fortune CEO's like Satya Nadella, McAfee's CEO Chris Young, Cisco's CIO Colin Seward along with organizations like ISSA, research firms like Gartner too shine light on it from time to time. This book put together all the possible information with regards to cybersecurity, why you should choose it, the need for cyber security and how can you be part of it and fill the cybersecurity talent gap bit by bit. Starting with the essential understanding of security and its needs, we will move to security domain changes and how artificial intelligence and machine learning are helping to secure systems. Later, this book will walk you through all the skills and tools that everyone who wants to work as security personal need to be aware of. Then, this book will teach readers how to think like an attacker and explore some advanced security methodologies. Lastly, this book will deep dive into how to build practice labs, explore real-world use cases and get acquainted with various cybersecurity certifications. By the end of this book, readers will be well-versed with the security domain and will be capable of making the right choices in the cybersecurity field. What you will learnGet an overview of what cybersecurity is and learn about the various faces of cybersecurity as well as identify domain that suits you bestPlan your transition into cybersecurity in an efficient and effective wayLearn how to build upon your existing skills and experience in order to prepare for your career in cybersecurityWho this book is for This book is targeted to any IT professional who is looking to venture in to the world cyber attacks and threats. Anyone with some understanding or IT infrastructure workflow will benefit from this book. Cybersecurity experts interested in enhancing their skill set will also find this book useful.

Hacking For Dummies - Kevin Beaver 2022-04-26

Learn to think like a hacker to secure your own systems and data Your smartphone, laptop, and desktop computer are more important to your life and business than ever before. On top of making your life easier and more productive, they hold sensitive information that should remain private. Luckily for all of us, anyone can learn powerful data privacy and security techniques to keep the bad guys on the outside where they belong. Hacking For Dummies takes you on an easy-to-follow cybersecurity voyage that will teach you the essentials of vulnerability and penetration testing so that you can find the holes in your network before the bad guys exploit them. You will learn to secure your Wi-Fi networks, lock down your latest Windows 11 installation, understand the security implications of remote work, and much more. You'll find out how to: Stay on top of the latest security weaknesses that could affect your business's security setup Use freely available testing tools to "penetration test" your network's security Use ongoing security checkups to continually ensure that your data is safe from hackers Perfect for small business owners, IT and security professionals, and employees who work remotely, Hacking For Dummies is a must-have resource for anyone who wants to keep their data safe.

Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document - OECD 2015-10-01

This OECD Recommendation and its Companion Document provide guidance for all stakeholders on the economic and social prosperity dimensions of digital security risk.

The Business Model Navigator - Oliver Gassmann 2014-11-10

A strong business model is the bedrock to business success. But all too often we fail to adapt, clinging to outdated models that are no longer delivering the results we need. The brains behind The Business Model Navigator have discovered that just 55 business models are responsible for 90% of the world's most successful businesses. These 55 models – from the Add-On model used by Ryanair to the Subscription model used by Spotify – provide the blueprints you need to revolutionise your business and drive powerful change. As well as providing a practical framework for adapting and innovating your business model, this book also includes each of the 55 models in a quick-read format that covers: What it is Who invented it and who uses it now When and how to apply it "An excellent toolkit for developing your business model." Dr Heinz Derenbach, CEO, Bosch Software Innovations

Network Security Tools - Nitesh Dhanjani 2005-04-04

If you're an advanced security professional, then you know that the battle to protect online privacy continues to rage on. Security chat rooms, especially, are resounding with calls for vendors to take more responsibility to release products that are more secure. In fact, with all the information and code that is passed on a daily basis, it's a fight that may never end. Fortunately, there are a number of open source security tools that give you a leg up in the battle.Often a security tool does exactly what you want, right out of the box. More frequently, you need to customize the tool to fit the needs of your network structure. Network Security Tools shows experienced administrators how to modify, customize, and extend popular open source security tools such as Nikto, Ettercap, and Nessus.This concise, high-end guide discusses the common customizations and extensions for these tools, then shows you how to write even more specialized attack and penetration reviews that are suited to your unique network environment. It also explains how tools like port scanners, packet injectors, network sniffers, and web assessment tools function.Some of the topics covered include: Writing your own network sniffers and packet injection tools Writing plugins for Nessus, Ettercap, and Nikto Developing exploits for Metasploit Code analysis for web applications Writing kernel modules for security applications, and understanding rootkits While many books on security are either tediously academic or overly sensational, Network Security Tools takes an even-handed and accessible approach that will let you quickly review the problem and implement new, practical solutions--without reinventing the wheel. In an age when security is critical, Network Security Tools is the resource you want at your side when locking down your network.

Hackers - Steven Levy 2010-05-19

This 25th anniversary edition of Steven Levy's classic book traces the exploits of the computer revolution's original hackers -- those brilliant and eccentric nerds from the late 1950s through the early '80s who took risks, bent the rules, and pushed the world in a radical new direction. With updated material from noteworthy hackers such as Bill Gates, Mark Zuckerberg, Richard Stallman, and Steve Wozniak, Hackers is a fascinating story that begins in early computer research labs and leads to the first home computers. Levy profiles the imaginative brainiacs who found clever and unorthodox solutions to computer engineering problems. They had a shared sense of values, known as "the hacker ethic," that still thrives today. Hackers captures a seminal period in recent history when underground activities blazed a trail for today's digital world, from MIT students finagling access to clunky computer-card machines to the DIY culture that spawned the Altair and the Apple

II.
Social Engineering - Christopher Hadnagy 2010-11-29
The first book to reveal and dissect the technical aspect of many social engineering maneuvers 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 unraveled 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 maneuvers that are aimed at deceiving unsuspecting victims, while it also addresses ways to prevent social engineering threats. Examines social engineering, the science of influencing a target to perform a desired task or divulge information Arms you with invaluable information about the many methods of trickery that hackers use in order to gather information with the intent of executing identity theft, fraud, or gaining computer system access Reveals vital steps for preventing social engineering threats Social Engineering: The Art of Human Hacking does its part to prepare you against nefarious hackers—now you can do your part by putting to good use the critical information within its pages.
Identity Attack Vectors - Morey J. Haber 2019-12-17
Discover how poor identity and privilege management can be leveraged to compromise accounts and credentials within an organization. Learn how role-based identity assignments, entitlements, and auditing strategies can be implemented to mitigate the threats leveraging accounts and identities and how to manage compliance for regulatory initiatives. As a solution, Identity Access Management (IAM) has emerged as the cornerstone of enterprise security. Managing accounts, credentials, roles, certification, and attestation reporting for all resources is now a security and compliance mandate. When identity theft and poor identity management is leveraged as an attack vector, risk and vulnerabilities increase exponentially. As cyber attacks continue to increase in volume and sophistication, it is not a matter of if, but when, your organization will have an incident. Threat actors target accounts, users, and their associated identities, to conduct their malicious activities through privileged attacks and asset vulnerabilities. Identity Attack Vectors details the risks associated with poor identity management practices, the techniques that threat actors and insiders leverage, and the operational best practices that organizations should adopt to protect against identity theft and account compromises, and to develop an effective identity governance program. What You Will Learn Understand the concepts behind an identity and how their associated credentials and accounts can be leveraged as an attack vector Implement an effective Identity Access Management (IAM) program to manage identities and roles, and provide certification for regulatory compliance See where identity management controls play a part of the cyber kill chain and how privileges should be managed as a potential weak link Build upon industry standards to integrate key identity management technologies into a corporate ecosystem Plan for a successful deployment, implementation scope, measurable risk reduction, auditing and discovery, regulatory reporting, and oversight based on real-world strategies to prevent identity attack vectors Who This Book Is For Management and implementers in IT operations, security, and auditing looking to understand and implement an identity access management program and manage privileges in these environments
What Is Cybersecurity? - Haq Kamar 2017-12-15
Inexperienced users of computers often jump at the chance to click colorful flashing ads on the sidebar and are also tempted to download files from sites not worthy of trust. In short, people need to learn how to stay safe online. This book will introduce readers to different types of online threats, including viruses and malware. They will learn how different dangers spread and some basic steps to stop or prevent them. Additionally, this book will illuminate the scary consequences of falling prey to those threats, such as having personal information stolen or deleted, and cyberstalking.
Days of Fire - Peter Baker 2013-10-22
In Days of Fire, Peter Baker, Chief White House Correspondent for The New York Times, takes us on a gripping and intimate journey through the eight years of the Bush and Cheney administration in a tour-de-force narrative of a dramatic and controversial presidency. Theirs was the most captivating American political partnership since Richard Nixon and Henry Kissinger: a bold and untested president and his seasoned, relentless vice president. Confronted by one crisis after another, they struggled to protect the country, remake the world, and define their own relationship along the way. In Days of Fire, Peter Baker chronicles the history of the most consequential presidency in modern times through the prism of its two most compelling characters, capturing the elusive and shifting alliance of George Walker Bush and Richard Bruce Cheney as no historian has done before. He brings to life with in-the-room immediacy all the drama of an era marked by devastating terror attacks, the Iraq War, Hurricane Katrina, and financial collapse. The real story of Bush and Cheney is a far more fascinating tale than the familiar suspicion that Cheney was the power behind the throne. Drawing on hundreds of interviews with key players, and thousands of pages of never-released notes, memos, and other internal documents, Baker paints a riveting portrait of a partnership that evolved dramatically over time, from the early days when Bush leaned on Cheney, making him the most influential vice president in history, to their final hours, when the two had grown so far apart they were clashing in the West Wing. Together and separately, they were tested as no other president and vice president have been, first on a bright September morning, an unforgettable “day of fire” just months into the presidency, and on countless days of fire over the course of eight tumultuous years. Days of Fire is a monumental and definitive work that will rank with the best of presidential histories. As absorbing as a thriller, it is eye-opening and essential reading.
Botnet Detection - Wenke Lee 2007-10-23
Botnets have become the platform of choice for launching attacks and committing fraud on the Internet. A better understanding of Botnets will help to coordinate and develop new technologies to counter this serious security threat. Botnet Detection: Countering the Largest Security Threat consists of chapters contributed by world-class leaders in this field, from the June 2006 ARO workshop on Botnets. This edited volume represents the state-of-the-art in research on Botnets.
Cybersecurity Expert - Daniel R. Faust 2017-07-15
With our use of technology increasing every day, it’s not surprising that our need for cybersecurity experts is also growing. In this informative text, readers will learn about why we need cybersecurity and what these security experts do to keep sensitive digital information safe. Students are introduced to the concept of computational thinking, as well as STEM concepts addressed in the Next Generation Science Standards. Informational diagrams and full-color photographs help students make connections with the text.
Cryptography and Public Key Infrastructure on the Internet - Klaus Schmeh 2006-01-04
A practical guide to Cryptography and its use in the Internet and other communication networks. This overview takes the reader through basic issues and on to more advanced concepts, to cover all levels of interest. Coverage includes all key mathematical concepts, standardisation, authentication, elliptic curve cryptography, and algorithm modes and protocols (including SSL, TLS, IPSec, SMIME, & PGP protocols). * Details what the risks on the internet are and how cryptography can help * Includes a chapter on interception which is unique amongst competing books in this field * Explains Public Key Infrastructures (PKIs) - currently the most important issue when using cryptography in a large organisation * Includes up-to-date referencing of people, organisations, books and Web sites and the latest information about recent acts and standards affecting encryption practice * Tackles the practical issues such as the difference between SSL and IPSec, which companies are active on the market and where to get further information
Hacking mit Metasploit - Michael Messner 2017-11-28
Metasploit ist ein Penetration-Testing-Werkzeug, das in der Toolbox eines jeden Pentesters zu finden ist. Dieses Buch stellt das Framework detailliert vor und zeigt, wie Sie es im Rahmen unterschiedlichster Penetrationstests einsetzen. Am Beispiel von Metasploit erhalten Sie einen umfassenden Einblick ins Penetration Testing. Sie lernen typische Pentesting-Tätigkeiten kennen und können nach der Lektüre komplexe, mehrstufige Angriffe vorbereiten, durchführen und protokollieren. Jeder dargestellte Exploit bzw. jedes dargestellte Modul wird anhand eines praktischen Anwendungsbeispiels in einer gesicherten Laborumgebung vorgeführt. Behandelt werden u.a. folgende Themen: • Komplexe, mehrstufige Penetrationstests • Post-Exploitation-Tätigkeiten • Metasploit-Erweiterungen • Webapplikationen, Datenbanken, Client-Side-Angriffe, IPv6 • Automatisierung mit Ruby-Skripten • Entwicklung eigener Exploits inkl. SEHExploits • Exploits für Embedded Devices entwickeln • Umgehung unterschiedlichster Sicherheitsumgebungen Die

dritte Auflage wurde überarbeitet und aktualisiert. Neu dabei: • Post-Exploitation-Tätigkeiten mit Railgun vereinfachen • Bad-Characters bei der Entwicklung von Exploits berücksichtigen • Den Vulnerable Service Emulator nutzen Vorausgesetzt werden fundierte Kenntnisse der Systemtechnik (Linux und Windows) sowie der Netzwerktechnik.

IT-Sicherheit - Roland Hellmann 2022-11-07

Das Buch erklärt die Grundlagen der IT-Sicherheit, wobei auch die wichtigsten Methoden der Kryptographie allgemein verständlich erklärt werden. Verfügbarkeit von Speichermedien und Daten, Internet-Sicherheit und Firewalls werden ausführlich behandelt, und aktuelle Themen der IoT-Sicherheit abgedeckt. Ferner betrachtet die 2. Auflage das Threat Modeling am Beispiel der Automotive Security.

Praktische Einführung in Hardware Hacking - Marcel Mangel 2019-12-16

Schwachstellen von IoT- und Smart-Home-Geräten aufdecken Hardware, Firmware und Apps analysieren und praktische Tests durchführen Zahlreiche Praxisbeispiele wie Analyse und Hacking elektronischer Türschlösser, smarter LED-Lampen u.v.m. Smarte Geräte sind allgegenwärtig und sie sind leicht zu hacken – umso mehr sind Reverse Engineers und Penetration Tester gefragt, um Schwachstellen aufzudecken und so Hacking-Angriffen und Manipulation vorzubeugen. In diesem Buch lernen Sie alle Grundlagen des Penetration Testings für IoT-Geräte. Die Autoren zeigen Schritt für Schritt, wie ein Penetrationstest durchgeführt wird: von der Einrichtung des Testlabors über die OSINT-Analyse eines Produkts bis hin zum Prüfen von Hard- und Software auf Sicherheitslücken – u.a. anhand des OWASP-Standards. Sie erfahren darüber hinaus, wie Sie die Firmware eines IoT-Geräts extrahieren, entpacken und dynamisch oder statisch analysieren. Auch die Analyse von Apps, Webapplikationen und Cloudfunktionen wird behandelt. Außerdem finden Sie eine Übersicht der wichtigsten IoT-Protokolle und ihrer Schwachstellen. Es werden nur grundlegende IT-Security-Kenntnisse (insbesondere in den Bereichen Netzwerk- und Applikationssicherheit) und ein sicherer Umgang mit Linux vorausgesetzt. Die notwendigen Elektronik- und Hardwaredesign-Grundlagen geben Ihnen die Autoren mit an die Hand. Aus dem Inhalt: Testumgebung einrichten Vorbereitende OSINT-Analyse Elektronik-Grundlagen Einführung in das Hardware-Design von IoT-Geräten: 8-/32-Bit-Controller Android Embedded Devices All-in-One SoC Hardware-Analyse und Extraktion von Firmware Dateisysteme von IoT-Geräten Statische und dynamische Firmware-Analyse IoT-Protokolle und ihre Schwachstellen: Bluetooth LE ZigBee MQTT App-Analyse anhand des OWASP-Standards Testen von Backend-Systemen, Webapplikationen und Cloud-Umgebungen

Raspberry Pi Cookbook - Simon Monk 2013-12-10

The world of Raspberry Pi is evolving quickly, with many new interface boards and software libraries becoming available all the time. In this cookbook, prolific hacker and author Simon Monk provides more than 200 practical recipes for running this tiny low-cost computer with Linux, programming it with Python, and hooking up sensors, motors, and other hardware--including Arduino. Make sure to check out 10 of the over 60 video recipes for this book at: http://razzpisampler.oreilly.com/ You can purchase all recipes at:

Personal Cybersecurity - Marvin Waschke 2017-01-12

Discover the most prevalent cyber threats against individual users of all kinds of computing devices. This book teaches you the defensive best practices and state-of-the-art tools available to you to repel each kind of threat. Personal Cybersecurity addresses the needs of individual users at work and at home. This book covers personal cybersecurity for all modes of personal computing whether on consumer-acquired or company-issued devices: desktop PCs, laptops, mobile devices, smart TVs, WiFi and Bluetooth peripherals, and IoT objects embedded with network-connected sensors. In all these modes, the frequency, intensity, and sophistication of cyberattacks that put individual users at risk are increasing in step with accelerating mutation rates of malware and cybercriminal delivery systems. Traditional anti-virus software and personal firewalls no longer suffice to guarantee personal security. Users who neglect to learn and adopt the new ways of protecting themselves in their work and private environments put themselves, their associates, and their companies at risk of inconvenience, violation, reputational damage, data corruption, data theft, system degradation, system destruction, financial harm, and criminal disaster. This book shows what actions to take to limit the harm and recover from the damage. Instead of laying down a code of "thou shalt not" rules that admit of too many exceptions and contingencies to be of much practical use, cloud expert Marvin Waschke equips you with the battlefield intelligence, strategic understanding, survival training, and proven tools you need to intelligently assess the security threats in your environment and most effectively secure yourself from attacks. Through instructive examples and scenarios, the author shows you how to adapt and apply best practices to your own particular circumstances, how to automate and routinize your personal cybersecurity, how to recognize security breaches and act swiftly to seal them, and how to recover losses and restore functionality when attacks succeed. What You'll Learn Discover how computer security works and what it can protect us from See how a typical hacker attack works Evaluate computer security threats to the individual user and corporate systems Identify the critical vulnerabilities of a computer connected to the Internet Manage your computer to reduce vulnerabilities to yourself and your employer Discover how the adoption of newer forms of biometric authentication affects you Stop your router and other online devices from being co-opted into disruptive denial of service attacks Who This Book Is For Proficient and technically knowledgeable computer users who are anxious about cybercrime and want to understand the technology behind both attack and defense but do not want to go so far as to become security experts. Some of this audience will be purely home users, but many will be executives, technical managers, developers, and members of IT departments who need to adopt personal practices for their own safety and the protection of corporate systems. Many will want to impart good cybersecurity practices to their colleagues. IT departments tasked with indoctrinating their users with good safety practices may use the book as training material.

Cybersecurity - Peter W. Singer 2014-03

Dependence on computers has had a transformative effect on human society. Cybernetics is now woven into the core functions of virtually every basic institution, including our oldest ones. War is one such institution, and the digital revolution's impact on it has been profound. The American military, which has no peer, is almost completely reliant on high-tech computer systems. Given the Internet's potential for full-spectrum surveillance and information disruption, the marshaling of computer networks represents the next stage of cyberwar. Indeed, it is upon us already. The recent Stuxnet episode, in which Israel fed a malignant computer virus into Iran's nuclear facilities, is one such example. Penetration into US government computer systems by Chinese hackers-presumably sponsored by the Chinese government-is another. Together, they point to a new era in the evolution of human conflict. In Cybersecurity and Cyerbwar: What Everyone Needs to Know, noted experts Peter W. Singer and Allan Friedman lay out how the revolution in military cybernetics occurred and explain where it is headed. They begin with an explanation of what cyberspace is before moving on to discussions of how it can be exploited and why it is so hard to defend. Throughout, they discuss the latest developments in military and security technology. Singer and Friedman close with a discussion of how people and governments can protect themselves. In sum, Cybersecurity and Cyerbwar is the definitive account on the subject for the educated general reader who wants to know more about the nature of war, conflict, and security in the twenty-first century.

The IoT Hacker's Handbook - Aditya Gupta 2019-03-30

Take a practioner’s approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture. You’ll review the architecture's central components, from hardware communication interfaces, such as UARTand SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware. As the IoT rises to one of the most popular tech trends, manufactures need to take necessary steps to secure devices and protect them from attackers. The IoT Hacker's Handbook breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely. What You’ll LearnPerform a threat model of a real-world IoT device and locate all possible attacker entry points Use reverse engineering of firmware binaries to identify security issues Analyze,assess, and identify security issues in exploited ARM and MIPS based binariesSniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee Who This Book is For Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

Mastering Python Forensics - Dr. Michael Spreitzenbarth 2015-10-30

Master the art of digital forensics and analysis with Python About This Book Learn to perform forensic analysis and investigations with the help

of Python, and gain an advanced understanding of the various Python libraries and frameworks Analyze Python scripts to extract metadata and investigate forensic artifacts The writers, Dr. Michael Spreitzenbarth and Dr. Johann Uhrmann, have used their experience to craft this hands-on guide to using Python for forensic analysis and investigations Who This Book Is For If you are a network security professional or forensics analyst who wants to gain a deeper understanding of performing forensic analysis with Python, then this book is for you. Some Python experience would be helpful. What You Will Learn Explore the forensic analysis of different platforms such as Windows, Android, and vSphere Semi-automatically reconstruct major parts of the system activity and time-line Leverage Python ctypes for protocol decoding Examine artifacts from mobile, Skype, and browsers Discover how to utilize Python to improve the focus of your analysis Investigate in volatile memory with the help of volatility on the Android and Linux platforms In Detail Digital forensic analysis is the process of examining and extracting data digitally and examining it. Python has the combination of power, expressiveness, and ease of use that makes it an essential complementary tool to the traditional, off-the-shelf digital forensic tools. This book will teach you how to perform forensic analysis and investigations by exploring the capabilities of various Python libraries. The book starts by explaining the building blocks of the Python programming language, especially ctypes in-depth, along with how to automate typical tasks in file system analysis, common correlation tasks to discover anomalies, as well as templates for investigations. Next, we'll show you cryptographic algorithms that can be used during forensic investigations to check for known files or to compare suspicious files with online services such as VirusTotal or Mobile-Sandbox. Moving on, you'll learn how to sniff on the network, generate and analyze network flows, and perform log correlation with the help of Python scripts and tools. You'll get to know about the concepts of virtualization and how virtualization influences IT forensics, and you'll discover how to perform forensic analysis of a jailbroken/rooted mobile device that is based on iOS or Android. Finally, the book teaches you how to analyze volatile memory and search for known malware samples based on YARA rules. Style and approach This easy-to-follow guide will demonstrate forensic analysis techniques by showing you how to solve real-word-scenarios step by step.

IoT-Hacking - Nitesh Dhanjani 2016-03-31

In Zukunft werden Milliarden "Dinge" über das Internet miteinander verbunden sein. Hierdurch entstehen jedoch auch gigantische Sicherheitsrisiken. In diesem Buch beschreibt der international renommierte IT-Sicherheitsexperte Nitesh Dhanjani, wie Geräte im Internet of Things von Angreifern missbraucht werden können – seien es drahtlose LED-Lampen, elektronische Türschlösser, Babyfone, Smart-TVs oder Autos mit Internetanbindung. Wenn Sie Anwendungen für Geräte entwickeln, die mit dem Internet verbunden sind, dann unterstützt Dhanjani Sie mit diesem Leitfaden bei der Erkennung und Behebung von Sicherheitslücken. Er erklärt Ihnen nicht nur, wie Sie Schwachstellen in IoT-Systemen identifizieren, sondern bietet Ihnen auch einen umfassenden Einblick in die Taktiken der Angreifer. In diesem Buch werden Sie • Design, Architektur und sicherheitstechnische Aspekte drahtloser Beleuchtungssysteme analysieren, • verstehen, wie elektronische Türschlösser geknackt werden, • Mängel im Sicherheitsaufbau von Babyfonen untersuchen, • die Sicherheitsfunktionen von Smart-Home-Geräten bewerten, • Schwachstellen von Smart-TVs kennenlernen, • Sicherheitslücken "intelligenter" Autos erforschen, • realistische Angriffsszenarios verstehen, die auf der gängigen Nutzung von IoT-Geräten durch Anwender beruhen. Darüber hinaus zeigt Ihnen Nitesh Dhanjani Prototyping-Methoden, die Sicherheitsfragen bereits bei den allerersten Entwürfen berücksichtigen. Schließlich erhalten Sie einen Ausblick auf neue Angriffsformen, denen IoTSysteme in Zukunft ausgesetzt sein werden. Stimmen zur Originalausgabe: "Dieses Buch enthüllt Sicherheitslücken, mit denen schon in naher Zukunft Milliarden vernetzter Geräte infiziert sein werden. Es bietet praktische Anleitungen zur Bewältigung aufkommender Sicherheitsrisiken für Verbraucher, Entwickler und Studierende gleichermaßen." Prof. em.

Effective Project Management - Robert K. Wysocki 2011-09-26

Expert guidance on ensuring project success—the latest edition! Many projects fail to deliver on time and within budget, and often-poor project management is to blame. If you're a project manager, the newest edition of this expert and top-selling book will help you avoid the pitfalls and manage projects successfully. Covering the major project management techniques including Traditional (Linear and Incremental), Agile (Iterative and Adaptive), and Extreme, this book lays out a comprehensive overview of all of the best-of-breed project management approaches and tools today. You'll learn how to use these approaches effectively to achieve better outcomes. Fresh topics in this new edition include critical chain project management, using the Requirements Management Lifecycle as a key driver, career and professional development for project managers, and more. This book is packed with step-by-step instruction and practical case studies, and a companion web site offers additional exercises and solutions. Gives new or veteran project managers a comprehensive overview of the best-of-breed project management approaches and tools today Shows readers, through step-by-step instruction and practical case studies, how to use these tools effectively Updated new edition adds new material on career and professional development for project managers, critical chain project management, and more If you're seeking to improve your professional project management skills, the latest edition of this popular, successful, and in-depth book is the place to start. Visit http://wysockiepm.com/ for support materials and to connect with the author.

Enabling Things to Talk - Alessandro Bassi 2013-10-28

The Internet of Things (IoT) is an emerging network superstructure that will connect physical resources and actual users. It will support an ecosystem of smart applications and services bringing hyper-connectivity to our society by using augmented and rich interfaces. Whereas in the beginning IoT referred to the advent of barcodes and Radio Frequency Identification (RFID), which helped to automate inventory, tracking and basic identification, today IoT is characterized by a dynamic trend toward connecting smart sensors, objects, devices, data and applications. The next step will be “cognitive IoT,” facilitating object and data re-use across application domains and leveraging hyper-connectivity, interoperability solutions and semantically enriched information distribution. The Architectural Reference Model (ARM), presented in this book by the members of the IoT-A project team driving this harmonization effort, makes it possible to connect vertically closed systems, architectures and application areas so as to create open interoperable systems and integrated environments and platforms. It constitutes a foundation from which software companies can capitalize on the benefits of developing consumer-oriented platforms including hardware, software and services. The material is structured in two parts. Part A introduces the general concepts developed for and applied in the ARM. It is aimed at end users who want to use IoT technologies, managers interested in understanding the opportunities generated by these novel technologies, and system architects who are interested in an overview of the underlying basic models. It also includes several case studies to illustrate how the ARM has been used in real-life scenarios. Part B then addresses the topic at a more detailed technical level and is targeted at readers with a more scientific or technical background. It provides in-depth guidance on the ARM, including a detailed description of a process for generating concrete architectures, as well as reference manuals with guidelines on how to use the various models and perspectives presented to create a concrete architecture. Furthermore, best practices and tips on how system engineers can use the ARM to develop specific IoT architectures for dedicated IoT solutions are illustrated and exemplified in reverse mapping exercises of existing standards and platforms.

Transnational Commercial and Consumer Law - Toshiyuki Kono 2018-08-27

This book explores current developments in transnational commercial and consumer law. It features essays written by leading experts, many of who have taken part in the negotiation and formulation of the international instruments they discuss here. The contributors look at issues arising from the profound changes that globalization is having on the legal norms governing commercial and consumer transactions, both domestic and transnational. They consider how relations between private actors, state regulators, and national courts are being completely reconfigured. This, in turn, generates pressures for legal harmonization and creates opportunities for new national and transnational legal norms and procedures to develop. The contributions address both the dynamics and the substance of these developments. Topics included are the UNCITRAL Model Law on secured transactions and on cross-border insolvency, the ICC Uniform Customs and Practices of Documentary Credits (UCP 600), and the dispute resolution mechanism and practices of the World Trade Organization. The content was formerly presented as papers at the 18th Biennial Meeting of the International Academy of Commercial and Consumer Law (the International Academy) at Kyushu University, Japan. Overall, this book provides readers with a solid theoretical foundation and strong familiarity with the practice of law and

international commerce, offering realistic and practical conclusions.

Liquid Reign - Karl-Heinz Hasliprinz 2018-05-06

Liquid Reign is a work of speculative fiction, imagineering a fairly liveable future in 2051, neither dys- nor utopian.Melting the boundaries between science and fiction into a novel format, each chapter provides links to the sources of inspiration influencing it - ranging from Jean Jacques Rousseau's social contract of 1762 to blockchain startups from 2018."A vertiginous rollercoaster of ideas and a unique take on the future of (un)governance, delivered with irrepressible, unruly energy."- Jamie King of the Pirates, Host "Steal this Show""Tim Reutemann has become one of my favorite big brain boys over the past few months. In his book Liquid Reign he explores the future of democracy and civics in a way I have never seen done before... "- TheBurgerkrieg, Edgy Youtuber"Liquid Reign is a SciFi Novel about technology and our future and AI an all sorts of awesome shit and how it's gonna affect our world"- Jarred "PiG" Krensel, Ex Pro-Starcraft Player and e-Sports commentator "Wooow, what a reading experience - truly immersive! A world with liquid democracy, artificial intelligence,universal basic income and a limit on wealth accumulation. After you've read the book, you have a feeling of a possible future."- Raphel Fasko, Mastermind of the Circular Economy

Practical IoT Hacking - Fotios Chantzis 2021-03-23

The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to: • Write a DICOM service scanner as an NSE module • Hack a microcontroller through the UART and SWD interfaces • Reverse engineer firmware and analyze mobile companion apps • Develop an NFC fuzzer using Proxmark3 • Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

Click Here to Kill Everybody - Bruce Schneier 2019-05-22

DAS INTERNET IST NICHT SICHER – FÜR KEINEN VON UNS Der weltweit bekannte IT-Sicherheitsexperte Bruce Schneier deckt die eklatanten Sicherheitslücken unserer hypervernetzten Welt auf. Identitäts- und Datendiebstahl sind dabei noch das geringste Risiko. Hacker können sogar die Kontrolle über Ihr Auto, Ihre Alarmanlage oder das nationale Stromnetz übernehmen, solange das Internet of Things nicht sicherer wird. Bruce Schneier zeigt in diesem Buch anhand beunruhigender und zugleich aufschlussreicher Fallbeispiele, wie leicht es für Hacker ist, Sicherheitslücken in Software und Protokollen auszunutzen und nahezu jedes technische Gerät unseres Alltags zu kompromittieren. Die Risiken sind unüberschaubar und können katastrophale Ausmaße annehmen. Dennoch haben Unternehmen und Regierungen bisher scheinbar kein großes Interesse daran, die IT-Sicherheit zu verbessern. Bruce Schneier beleuchtet ausführlich, wie die aktuellen Sicherheitsmängel entstanden sind und welche enormen Auswirkungen sie in Zukunft auf unser tägliches Leben haben könnten. Er fordert Regierungen mit konkreten Handlungsvorschlägen auf, das Internet of Things zukünftig verantwortungsvoll zu regulieren, und macht deutlich, was getan werden muss, um die Sicherheitslücken zu schließen. Stimmen zum Buch: »Schneiers Buch zeigt ernüchternd und aufschlussreich, wie es zu den Sicherheitsmängeln kommen konnte, die durch die zunehmende Ausbreitung des Internets auf alle Lebensbereiche entstanden sind, und was man dagegen tun sollte (und wahrscheinlich nicht tun wird).« – NATURE »Schneier führt dem Leser eindrucksvoll die massiven Hackerangriffe der Vergangenheit vor Augen – und welche er noch kommen sieht. […] Er stellt detaillierte Lösungsansätze vor, die für Politiker auf der ganzen Welt Pflichtlektüre sein sollten.« – FINANCIAL TIMES

The Basics of Cyber Safety - John Sammons 2016-08-20

The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy presents modern tactics on how to secure computer and mobile devices, including what behaviors are safe while surfing, searching, and interacting with others in the virtual world. The book's author, Professor John Sammons, who teaches information security at Marshall University, introduces readers to the basic concepts of protecting their computer, mobile devices, and data during a time that is described as the most connected in history. This timely resource provides useful information for readers who know very little about the basic principles of keeping the devices they are connected to—or themselves—secure while online. In addition, the text discusses, in a non-technical way, the cost of connectedness to your privacy, and what you can do to it, including how to avoid all kinds of viruses, malware, cybercrime, and identity theft. Final sections provide the latest information on safe computing in the workplace and at school, and give parents steps they can take to keep young kids and teens safe online. Provides the most straightforward and up-to-date guide to cyber safety for anyone who ventures online for work, school, or personal use Includes real world examples that demonstrate how cyber criminals commit their crimes, and what users can do to keep their data safe

Arduino for the Cloud - Claus Kuhnel 2015-05-19

Arduino for the Cloud considers the Arduino Yún and the Dragino Yún Shield as components closing the gap between a typical microcontroller application and connection to the cloud. Arduino Yún combines the classic Arduino with an Atheros AR9331 system-on-a-chip (SoC) for wireless access points and routers platforms, which uses the Linux distribution Linino (OpenWRT) operating system. The Dragino Yun Shield expands any Arduino with network capabilities by the Atheros AR9331.The combination of microcontroller and Linux device supports the whole chain from sensor to software applications in the cloud by hardware and software. This book deals with the Arduino and the Linux device and their interaction, without the need of detailed Linux knowledge.

Arduino For Dummies - John Nussey 2013-04-29

The quick, easy way to leap into the fascinating world ofphysical computing This is no ordinary circuit board. Arduino allows anyone,whether you're an artist, designer, programmer or hobbyist, tolearn about and play with electronics. Through this book you learnhow to build a variety of circuits that can sense or control thingsin the real world. Maybe you'll prototype your own product orcreate a piece of interactive artwork? This book equips you witheverything you'll need to build your own Arduino project, but whatyou make is up to you! If you're ready to bring your ideas into thereal world or are curious about the possibilities, this book is foryou. ? Learn by doing ? start building circuits and programmingyour Arduino with a few easy to follow examples - rightaway! ? Easy does it ? work through Arduino sketches line by linein plain English, to learn of how a they work and how to write yourown ? Solder on! ? Only ever used a breadboard in the kitchen?Don't know your soldering iron from a curling iron? No problem,you'll be prototyping in no time ? Kitted out ? discover new and interesting hardware to makeyour Arduino into anything from a mobile phone to a geigercounter! ? Become an Arduino savant ? learn all about functions,arrays, libraries, shields and other tools of the trade to takeyour Arduino project to the next level. ? Get social ? teach your Arduino to communicate withsoftware running on a computer to link the physical world with thevirtual world It's hardware, it's software, it's fun! Start building the nextcool gizmo with Arduino and Arduino For Dummies.

Understanding Security Issues - Scott Donaldson 2018-12-17

With the threats that affect every computer, phone or other device connected to the internet, security has become a responsibility not just for law enforcement authorities or business leaders, but for every individual. Your family, information, property, and business must be protected from cybercriminals in the office, at home, on travel, and in the cloud. Understanding Security Issues provides a solid understanding of the threats, and focuses on useful tips and practices for protecting yourself, all the time, everywhere and anywhere you go. This book discusses security awareness issues and how you can take steps to reduce the risk of becoming a victim: The threats that face every individual and business, all the time. Specific indicators of threats so that you understand when you might be attacked and what to do if they occur. The security mindset and good security practices. Assets that need to be protected at work and at home. Protecting yourself and your business at work. Protecting yourself and your family at home. Protecting yourself and your assets on travel.