Devsecops The Tao Of Security Science Rsa Conference

This is likewise one of the factors by obtaining the soft documents of this **Devsecops The Tao Of Security Science Rsa Conference** by online. You might not require more era to spend to go to the book introduction as with ease as search for them. In some cases, you likewise reach not discover the declaration Devsecops The Tao Of Security Science Rsa Conference that you are looking for. It will categorically squander the time.

However below, similar to you visit this web page, it will be as a result completely easy to acquire as well as download lead Devsecops The Tao Of Security Science Rsa Conference

It will not agree to many time as we run by before. You can attain it even if acquit yourself something else at house and even in your workplace. thus easy! So, are you question? Just exercise just what we find the money for under as well as review **Devsecops The Tao Of Security Science Rsa Conference** what you considering to read!

System-Level Synthesis - Ahmed Amine Jerraya 2012-12-06
System-Level Synthesis deals with the concurrent design of electronic applications, including both hardware and software. The issue has become the bottleneck in the design of electronic systems, including both hardware and software, in several major industrial fields, including telecommunications, automotive and aerospace engineering. The major difficulty with the subject is that it demands contributions from several research fields, including system specification, system architecture, hardware design, and software design. Most existing book cover well only a few aspects of system-level synthesis. The present volume presents a comprehensive discussion of all the aspects of system-level synthesis. Each topic is covered by a contribution written by an international authority on the subject.
Moving Forward - Terry Bills 2021-10-26
Discover how GIS and location intelligence are helping transportation organizations strengthen their vital infrastructures with Moving Forward: Applying GIS for Transportation.
Mastering OpenCV with Practical Computer Vision Projects - Daniel Lélis Baggio 2012-12-03
Each chapter in the book is an individual project and each project is constructed with step-by-step instructions, clearly explained code, and includes the necessary screenshots. You should have basic OpenCV and C/C++ programming experience before reading this book, as it is aimed at Computer Science graduates, researchers, and computer vision experts widening their expertise.
Adaptive Dynamic Programming: Single and Multiple Controllers - Ruizhuo Song 2018-12-28
This book presents a class of novel optimal control methods and games schemes based on adaptive dynamic programming techniques. For systems with one control input, the ADP-based optimal control is designed for different objectives, while for systems with multi-players, the optimal control inputs are proposed based on games. In order to verify the effectiveness of the proposed methods, the book analyzes the properties of the adaptive dynamic programming methods, including convergence of the iterative value functions and the stability of the system under the iterative control laws. Further, to substantiate the mathematical analysis, it presents various application examples, which provide reference to real-world practices.
Geary's Guide to the World's Great Aphorists - James Geary 2008-12-08
Both an expert and a collector, James Geary has devoted his life to aphorisms-and the last few years to organizing, indexing, and even translating them. The result is Geary's Guide, featuring aphorists like Voltaire, Twain, Shakespeare, Nietzsche, Woody Allen, Muhammad Ali, Emily Dickinson, and Mae West, as well as international practitioners appearing in English for the first time. But it is more than just a conventional anthology. It is also an encyclopedia, containing brief biographies of each author in addition to a selection of his or her aphorisms. The book is a field guide, too, with aphorists organized into eight different "species," such as Comics, Critics & Satirists; Icons & Iconoclasts; and Painters & Poets. The book's two indexes-by author and by subject-make it easily searchable, while its unique organizational structure and Geary's lively biographical entries set it apart from all previous reference works. A perfect follow-up to Geary's New York Times bestseller The World in a Phrase, Geary's Guide is eminently suitable for browsing or for sustained reading. A comprehensive guide to our most intimate, idiosyncratic literary form, the book is an indispensable tool for writers and public speakers as well as essential reading for all language lovers.
Microsoft Azure Network Security - Nicholas DiCola 2021-06-09
Following the same approach as Microsoft Press's widely-praised Microsoft Azure Sentinel and Microsoft Azure Security Center, the authors begin with a thoughtful overview of the network security domain and its importance in the cloud. Next, they present detailed chapters on cloud-native solutions for firewalling, DDOS, WAF, and other services, showing how cloud professionals can successfully deploy them within a best practice architecture. Next, they walk through integrating key third parties, successfully monitoring network security services, and combining all components in a cohesive, "wholistic" network security strategy that can serve as the basis for security and compliance for years to come. No matter how large, small, simple, or complex your Azure environment is, Microsoft Azure Network Security will help you protect what matters most.
Beyond The Phoenix Project - Gene Kim 2018-02-27
This is a companion transcript of the audio series, Beyond The Phoenix Project, intended to be used for reference and to enable further research of cited material, and not as a standalone work. In the audio series, Gene Kim and John Willis present a nine-part discussion that includes an oral history of the DevOps movement, as well as discussions around pivotal figures and philosophies that DevOps draws upon, from Goldratt to Deming; from Lean to Safety Culture to Learning Organizations.The book is a great way for listeners to take an even deeper dive into topics relevant to DevOps and leading technology organizations.
Incident Response - Chris Prosise 2001
Incident response is a multidisciplinary science that resolves computer crime and complex legal issues, chronological methodologies and technical computer techniques. The commercial industry has embraced and adopted technology that detects hacker incidents. Companies are swamped with real attacks, yet very few have any methodology or knowledge to resolve these attacks. Incident Response: Investigating Computer Crime will be the only book on the market that provides the information on incident response that network professionals need to conquer attacks.
Schneier on Security - Bruce Schneier 2009-03-16
Presenting invaluable advice from the world?s most famous computer security expert, this intensely readable collection features some of the most insightful and informative coverage of the strengths and weaknesses of computer security and the price people pay -- figuratively and literally -- when security fails. Discussing the issues surrounding things such as airplanes, passports, voting machines, ID cards, cameras, passwords, Internet banking, sporting events, computers, and castles, this book is a must-read for anyone who values security at any level -- business, technical, or personal.
Modern Telemetry - Ondrej Krejcar 2011-10-05
Telemetry is based on knowledge of various disciplines like Electronics, Measurement, Control and Communication along with their combination. This fact leads to a need of studying and understanding of these principles before the usage of Telemetry on selected problem solving. Spending time is however many times returned in form of obtained data or knowledge which telemetry system can provide. Usage of telemetry can be found in many areas from military through biomedical to real medical applications.

Modern way to create a wireless sensors remotely connected to central system with artificial intelligence provide many new, sometimes unusual ways to get a knowledge about remote objects behaviour. This book is intended to present some new up to date accesses to telemetry problems solving by use of new sensors conceptions, new wireless transfer or communication techniques, data collection or processing techniques as well as several real use case scenarios describing model examples. Most of book chapters deals with many real cases of telemetry issues which can be used as a cookbooks for your own telemetry related problems.

The Tao of Network Security Monitoring - Richard Bejtlich 2004-07-12

"The book you are about to read will arm you with the knowledge you need to defend your network from attackers—both the obvious and the not so obvious.... If you are new to network security, don't put this book back on the shelf! This is a great book for beginners and I wish I had access to it many years ago. If you've learned the basics of TCP/IP protocols and run an open source or commercial IDS, you may be asking 'What's next?' If so, this book is for you." —Ron Gula, founder and CTO, Tenable Network Security, from the Foreword "Richard Bejtlich has a good perspective on Internet security—one that is orderly and practical at the same time. He keeps readers grounded and addresses the fundamentals in an accessible way." —Marcus Ranum, TruSecure "This book is not about security or network monitoring: It's about both, and in reality these are two aspects of the same problem. You can easily find people who are security experts or network monitors, but this book explains how to master both topics." —Luca Deri, ntop.org "This book will enable security professionals of all skill sets to improve their understanding of what it takes to set up, maintain, and utilize a successful network intrusion detection strategy." —Kirby Kuehl, Cisco Systems Every network can be compromised. There are too many systems, offering too many services, running too many flawed applications. No amount of careful coding, patch management, or access control can keep out every attacker. If prevention eventually fails, how do you prepare for the intrusions that will eventually happen? Network security monitoring (NSM) equips security staff to deal with the inevitable consequences of too few resources and too many responsibilities. NSM collects the data needed to generate better assessment, detection, and response processes—resulting in decreased impact from unauthorized activities. In The Tao of Network Security Monitoring , 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. Inside, you will find in-depth information on the following areas. The NSM operational framework and deployment considerations. How to use a variety of open-source tools—including Sguil, Argus, and Ethereal—to mine network traffic for full content, session, statistical, and alert data. Best practices for conducting emergency NSM in an incident response scenario, evaluating monitoring vendors, and deploying an NSM architecture. Developing and applying knowledge of weapons, tactics, telecommunications, system administration, scripting, and programming for NSM. The best tools for generating arbitrary packets, exploiting flaws, manipulating traffic, and conducting reconnaissance. Whether you are new to network intrusion detection and incident response, or a computer-security veteran, this book will enable you to quickly develop and apply the skills needed to detect, prevent, and respond to new and emerging threats.

Getting Started with Couchbase Server - M. C. Brown 2012

Do you know what to do if your web application goes viral and usage suddenly explodes? This concise guide introduces you to Couchbase Server, an extremely fast NoSQL database that automatically distributes data across a cluster of commodity servers or virtual machines. You'll learn hands-on how to build a Couchbase cluster without changing your application, and how to expand your database on the fly without interrupting service. Discover how this open source server can help your application gain scalability and performance. Learn how the server's architecture affects the way you build and deploy your database Store data without defining a data structure—and retrieve it without complex queries or query languages Use a formula to estimate your cluster size requirements Set up individual nodes through a browser, command line, or REST API Enable your application to read and write data with sub-millisecond latency through managed object caching Get a quick guide to building applications that integrate Couchbase's core protocol Identify problems in your cluster with the web console Expand or shrink your cluster, handle failovers, and back up data

A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years - Sergio Flesca 2017-05-29

This book offers readers a comprehensive guide to the evolution of the database field from its earliest stages up to the present—and from classical relational database management systems to the current Big Data metaphor. In particular, it gathers the most significant research from the Italian database community that had relevant intersections with international projects. Big Data technology is currently dominating both the market and research. The book provides readers with a broad overview of key research efforts in modelling, querying and analysing data, which, over the last few decades, have became massive and heterogeneous areas.

Building Micro-Frontends - Luca Mezzalira 2021-11-17

What's the answer to today's increasingly complex web applications? Micro-frontends. Inspired by the microservices model, this approach lets you break interfaces into separate features managed by different teams of developers. With this practical guide, Luca Mezzalira shows software architects, tech leads, and software developers how to build and deliver artifacts atomically rather than use a big bang deployment. You'll learn how micro-frontends enable your team to choose any library or framework. This gives your organization technical flexibility and allows you to hire and retain a broad spectrum of talent. Micro-frontends also support distributed or colocated teams more efficiently. Pick up this book and learn how to get started with this technological breakthrough right away. Explore available frontend development architectures Learn how microservice principles apply to frontend development Understand the four pillars for creating a successful micro-frontend architecture Examine the benefits and pitfalls of existing micro-frontend architectures Learn principles and best practices for creating successful automation strategies Discover patterns for integrating micro-frontend architectures using microservices or a monolith API layer

Research Anthology on Artificial Intelligence Applications in Security - Management Association, Information Resources 2020-11-27

As industries are rapidly being digitalized and information is being more heavily stored and transmitted online, the security of information has become a top priority in securing the use of online networks as a safe and effective platform. With the vast and diverse potential of artificial intelligence (AI) applications, it has become easier than ever to identify cyber vulnerabilities, potential threats, and the identification of solutions to these unique problems. The latest tools and technologies for AI applications have untapped potential that conventional systems and human security systems cannot meet, leading AI to be a frontrunner in the fight against malware, cyber-attacks, and various security issues. However, even with the tremendous progress AI has made within the sphere of security, it’s important to understand the impacts, implications, and critical issues and challenges of AI applications along with the many benefits and emerging trends in this essential field of security-based research. Research Anthology on Artificial Intelligence Applications in Security seeks to address the fundamental advancements and technologies being used in AI applications for the security of digital data and information. The included chapters cover a wide range of topics related to AI in security stemming from the development and design of these applications, the latest tools and technologies, as well as the utilization of AI and what challenges and impacts have been discovered along the way. This resource work is a critical exploration of the latest research on security and an overview of how AI has impacted the field and will continue to advance as an essential tool for security, safety, and privacy online. This book is ideally intended for cyber security analysts, computer engineers, IT specialists, practitioners, stakeholders, researchers, academicians, and students interested in AI applications in the realm of security research.

Data Pipelines with Apache Airflow - Julian de Ruiter 2021-04-05

"An Airflow bible. Useful for all kinds of users, from novice to expert." - Rambabu Posa, Sai Aashika Consultancy Data Pipelines with Apache Airflow teaches you how to build and maintain effective data pipelines. A successful pipeline moves data efficiently, minimizing pauses and blockages between tasks, keeping every process along the way operational. Apache Airflow provides a single customizable environment for building and managing data pipelines, eliminating the need for a hodgepodge collection of tools, snowflake code, and homegrown processes. Using real-world scenarios and examples, Data Pipelines

with Apache Airflow teaches you how to simplify and automate data pipelines, reduce operational overhead, and smoothly integrate all the technologies in your stack. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Data pipelines manage the flow of data from initial collection through consolidation, cleaning, analysis, visualization, and more. Apache Airflow provides a single platform you can use to design, implement, monitor, and maintain your pipelines. Its easy-to-use UI, plug-and-play options, and flexible Python scripting make Airflow perfect for any data management task. About the book Data Pipelines with Apache Airflow teaches you how to build and maintain effective data pipelines. You'll explore the most common usage patterns, including aggregating multiple data sources, connecting to and from data lakes, and cloud deployment. Part reference and part tutorial, this practical guide covers every aspect of the directed acyclic graphs (DAGs) that power Airflow, and how to customize them for your pipeline's needs. What's inside Build, test, and deploy Airflow pipelines as DAGs Automate moving and transforming data Analyze historical datasets using backfilling Develop custom components Set up Airflow in production environments About the reader For DevOps, data engineers, machine learning engineers, and sysadmins with intermediate Python skills. About the author Bas Harenslak and Julian de Ruiter are data engineers with extensive experience using Airflow to develop pipelines for major companies. Bas is also an Airflow committer. Table of Contents PART 1 - GETTING STARTED 1 Meet Apache Airflow 2 Anatomy of an Airflow DAG 3 Scheduling in Airflow 4 Templating tasks using the Airflow context 5 Defining dependencies between tasks PART 2 - BEYOND THE BASICS 6 Triggering workflows 7 Communicating with external systems 8 Building custom components 9 Testing 10 Running tasks in containers PART 3 - AIRFLOW IN PRACTICE 11 Best practices 12 Operating Airflow in production 13 Securing Airflow 14 Project: Finding the fastest way to get around NYC PART 4 - IN THE CLOUDS 15 Airflow in the clouds 16 Airflow on AWS 17 Airflow on Azure 18 Airflow in GCP

Microsoft Azure Security Center - Yuri Diogenes 2018-06-04

Discover high-value Azure security insights, tips, and operational optimizations This book presents comprehensive Azure Security Center techniques for safeguarding cloud and hybrid environments. Leading Microsoft security and cloud experts Yuri Diogenes and Dr. Thomas Shinder show how to apply Azure Security Center's full spectrum of features and capabilities to address protection, detection, and response in key operational scenarios. You'll learn how to secure any Azure workload, and optimize virtually all facets of modern security, from policies and identity to incident response and risk management. Whatever your role in Azure security, you'll learn how to save hours, days, or even weeks by solving problems in most efficient, reliable ways possible. Two of Microsoft's leading cloud security experts show how to: • Assess the impact of cloud and hybrid environments on security, compliance, operations, data protection, and risk management • Master a new security paradigm for a world without traditional perimeters • Gain visibility and control to secure compute, network, storage, and application workloads • Incorporate Azure Security Center into your security operations center • Integrate Azure Security Center with Azure AD Identity Protection Center and third-party solutions • Adapt Azure Security Center's built-in policies and definitions for your organization • Perform security assessments and implement Azure Security Center recommendations • Use incident response features to detect, investigate, and address threats • Create high-fidelity fusion alerts to focus attention on your most urgent security issues • Implement application whitelisting and just-in-time VM access • Monitor user behavior and access, and investigate compromised or misused credentials • Customize and perform operating system security baseline assessments • Leverage integrated threat intelligence to identify known bad actors

Nobody's Victim - Carrie Goldberg 2019-08-13

Nobody's Victim is an unflinching look at a hidden world most people don't know exists—one of stalking, blackmail, and sexual violence, online and off—and the incredible story of how one lawyer, determined to fight back, turned her own hell into a revolution. "We are all a moment away from having our life overtaken by somebody hell-bent on our destruction." That grim reality—gleaned from personal experience and twenty years of trauma work—is a fundamental principle of Carrie Goldberg's cutting-edge victims' rights law firm. Riveting and an essential timely conversation-starter, Nobody's Victim invites readers to join Carrie on the front lines of the war against sexual violence and privacy violations as she fights for revenge porn and sextortion laws, uncovers major Title IX violations, and sues the hell out of tech companies, schools, and powerful sexual predators. Her battleground is the courtroom; her crusade is to transform clients from victims into warriors. In gripping detail, Carrie shares the diabolical ways her clients are attacked and how she, through her unique combination of advocacy, badass relentlessness, risk-taking, and client-empowerment, pursues justice for them all. There are stories about a woman whose ex-boyfriend made fake bomb threats in her name and caused a national panic; a fifteen-year-old girl who was sexually assaulted on school grounds and then suspended when she reported the attack; and a man whose ex-boyfriend used a dating app to send more than 1,200 men to ex's home and work for sex. With breathtaking honesty, Carrie also shares her own shattering story about why she began her work and the uphill battle of building a business. While her clients are a diverse group—from every gender, sexual orientation, age, class, race, religion, occupation, and background—the offenders are not. They are highly predictable. In this book, Carrie offers a taxonomy of the four types of offenders she encounters most often at her firm: assholes, psychos, pervs, and trolls. "If we recognize the patterns of these perpetrators," she explains, "we know how to fight back." Deeply personal yet achingly universal, Nobody's Victim is a bold and much-needed analysis of victim protection in the era of the Internet. This book is an urgent warning of a coming crisis, a predictor of imminent danger, and a weapon to take back control and protect ourselves—both online and off.

Kingpin - Kevin Poulsen 2012-02-07

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. The word spread through the hacking underground like some unstoppable new virus: Someone—some brilliant, audacious crook—had just staged a hostile takeover of an online criminal network that siphoned billions of dollars from the US economy. The FBI rushed to launch an ambitious undercover operation aimed at tracking down this new kingpin; other agencies around the world deployed dozens of moles and double agents. Together, the cybercops lured numerous unsuspecting hackers into their clutches. . . . Yet at every turn, their main quarry displayed an uncanny ability to sniff out their snitches and see through their plots. The culprit they sought was the most unlikely of criminals: a brilliant programmer with a hippie ethic and a supervillain's double identity. As prominent "white-hat" hacker Max "Vision" Butler, he was a celebrity throughout the programming world, even serving as a consultant to the FBI. But as the black-hat "Iceman," he found in the world of data theft an irresistible opportunity to test his outsized abilities. He infiltrated thousands of computers around the country, sucking down millions of credit card numbers at will. He effortlessly hacked his fellow hackers, stealing their ill-gotten gains from under their noses. Together with a smooth-talking con artist, he ran a massive real-world crime ring. And for years, he did it all with seeming impunity, even as countless rivals ran afoul of police. Yet as he watched the fraudsters around him squabble, their ranks riddled with infiltrators, their methods inefficient, he began to see in their dysfunction the ultimate challenge: He would stage his coup and fix what was broken, run things as they should be run—even if it meant painting a bull's-eye on his forehead. Through the story of this criminal's remarkable rise, and of law enforcement's quest to track him down, Kingpin lays bare the workings of a silent crime wave still affecting millions of Americans. In these pages, we are ushered into vast online-fraud supermarkets stocked with credit card numbers, counterfeit checks, hacked bank accounts, dead drops, and fake passports. We learn the workings of the numerous hacks—browser exploits, phishing attacks, Trojan horses, and much more—these fraudsters use to ply their trade, and trace the complex routes by which they turn stolen data into millions of dollars. And thanks to Poulsen's remarkable access to both cops and criminals, we step inside the quiet, desperate arms race that law enforcement continues to fight with these scammers today. Ultimately, Kingpin is a journey into an underworld of startling scope and power, one in which ordinary American teenagers work hand in hand with murderous Russian mobsters and where a simple Wi-Fi connection can unleash a torrent of gold worth millions.

Security+ Guide to Network Security Fundamentals - Mark Ciampa 2012-07-27

Reflecting the latest trends and developments from the information security field, best-selling Security+ Guide to Network Security Fundamentals, Fourth Edition, provides a complete introduction to practical

network and computer security and maps to the CompTIA Security+ SY0-301 Certification Exam. The text covers the fundamentals of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. The updated edition includes 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. The new edition features activities that link to the Information Security Community Site, which offers video lectures, podcats, discussion boards, additional hands-on activities and more to provide a wealth of resources and up-to-the minute information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Threat Modeling - Adam Shostack 2014-02-12

The only security book to be chosen as a Dr. Dobbs Jolt Award Finalist since Bruce Schneier's Secrets and Lies and Applied Cryptography! 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. Systems security managers, you'll find tools and a framework for structured thinking about what can go wrong. Software developers, you'll appreciate the jargon-free and accessible introduction to this essential skill. Security professionals, you'll learn to discern changing threats and discover the easiest ways to adopt a structured approach to threat modeling. Provides a unique how-to for security and software developers who need to design secure products and systems and test their designs Explains how to threat model and explores various threat modeling approaches, such as asset-centric, attacker-centric and software-centric Provides effective approaches and techniques that have been proven at Microsoft and elsewhere Offers actionable how-to advice not tied to any specific software, operating system, or programming language Authored by a Microsoft professional who is one of the most prominent threat modeling experts in the world As more software is delivered on the Internet or operates on Internet-connected devices, the design of secure software is absolutely critical. Make sure you're ready with Threat Modeling: Designing for Security.

Exam Ref SC-200 Microsoft Security Operations Analyst - Yuri Diogenes 2021-09-08

Prepare for Microsoft Exam SC-200--and help demonstrate your real-world mastery of skills and knowledge required to work with stakeholders to secure IT systems, and to rapidly remediate active attacks. Designed for Windows administrators, Exam Ref focuses on the critical thinking and decision-making acumen needed for success at the Microsoft Certified Associate level. Focus on the expertise measured by these objectives: Mitigate threats using Microsoft 365 Defender Mitigate threats using Azure Defender Mitigate threats using Azure Sentinel This Microsoft Exam Ref: Organizes its coverage by exam objectives Features strategic, what-if scenarios to challenge you Assumes you have experience with threat management, monitoring, and/or response in Microsoft 365 environments About the Exam Exam SC-200 focuses on knowledge needed to detect, investigate, respond, and remediate threats to productivity, endpoints, identity, and applications; design and configure Azure Defender implementations; plan and use data connectors to ingest data sources into Azure Defender and Azure Sentinel; manage Azure Defender alert rules; configure automation and remediation; investigate alerts and incidents; design and configure Azure Sentinel workspaces; manage Azure Sentinel rules and incidents; configure SOAR in Azure Sentinel; use workbooks to analyze and interpret data; and hunt for threats in the Azure Sentinel portal. About Microsoft Certification Passing this exam fulfills your requirements for the Microsoft 365 Certified: Security Operations Analyst Associate certification credential, demonstrating your ability to collaborate with organizational stakeholders to reduce organizational risk, advise on threat protection improvements, and address violations of organizational policies. See full details at: microsoft.com/learn

Offensive Countermeasures - John Strand 2013-07-08

Tired of playing catchup with hackers? Does it ever seem they have all of the cool tools? Does it seem like defending a network is just not fun? This books introduces new cyber-security defensive tactics to annoy attackers, gain attribution and insight on who and where they are. It discusses how to attack attackers in a way which is legal and incredibly useful.

Game Hacking - Nick Cano 2016-07-01

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

Microsoft Azure Sentinel - Yuri Diogenes 2020-02-25

Microsoft Azure Sentinel Plan, deploy, and operate Azure Sentinel, Microsoft’s advanced cloud-based SIEM Microsoft’s cloud-based Azure Sentinel helps you fully leverage advanced AI to automate threat identification and response – without the complexity and scalability challenges of traditional Security Information and Event Management (SIEM) solutions. Now, three of Microsoft’s leading experts review all it can do, and guide you step by step through planning, deployment, and daily operations. Leveraging in-the-trenches experience supporting early customers, they cover everything from configuration to data ingestion, rule development to incident management… even proactive threat hunting to disrupt attacks before you’re exploited. Three of Microsoft’s leading security operations experts show how to: • Use Azure Sentinel to respond to today’s fast-evolving cybersecurity environment, and leverage the benefits of its cloud-native architecture • Review threat intelligence essentials: attacker motivations, potential targets, and tactics, techniques, and procedures • Explore Azure Sentinel components, architecture, design considerations, and initial configuration • Ingest alert log data from services and endpoints you need to monitor • Build and validate rules to analyze ingested data and create cases for investigation • Prevent alert fatigue by projecting how many incidents each rule will generate • Help Security Operation Centers (SOCs) seamlessly manage each incident’s lifecycle • Move towards proactive threat hunting: identify sophisticated threat behaviors and disrupt cyber kill chains before you’re exploited • Do more with data: use programmable Jupyter notebooks and their libraries for machine learning, visualization, and data analysis • Use Playbooks to perform Security Orchestration, Automation and Response (SOAR) • Save resources by automating responses to low-level events • Create visualizations to spot trends, identify or clarify relationships, and speed decisions • Integrate with partners and other third-parties, including Fortinet, AWS, and Palo Alto

The Ethics of Cybersecurity - Markus Christen 2020-02-10

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

Cyber-Physical Security - Robert M. Clark 2016-08-10

This book focuses on the vulnerabilities of state and local services to cyber-threats and suggests possible

protective action that might be taken against such threats. Cyber-threats to U.S. critical infrastructure are of growing concern to policymakers, managers and consumers. Information and communications technology (ICT) is ubiquitous and many ICT devices and other components are interdependent; therefore, disruption of one component may have a negative, cascading effect on others. Cyber-attacks might include denial of service, theft or manipulation of data. Damage to critical infrastructure through a cyber-based attack could have a significant impact on the national security, the economy, and the livelihood and safety of many individual citizens. Traditionally cyber security has generally been viewed as being focused on higher level threats such as those against the internet or the Federal government. Little attention has been paid to cyber-security at the state and local level. However, these governmental units play a critical role in providing services to local residents and consequently are highly vulnerable to cyber-threats. The failure of these services, such as waste water collection and water supply, transportation, public safety, utility services, and communication services, would pose a great threat to the public. Featuring contributions from leading experts in the field, this volume is intended for state and local government officials and managers, state and Federal officials, academics, and public policy specialists.

Writing Secure Code - Michael Howard 2003

Covers topics such as the importance of secure systems, threat modeling, canonical representation issues, solving database input, denial-of-service attacks, and security code reviews and checklists.

Machine Learning and Security - Clarence Chio 2018-01-26

Can machine learning techniques solve our computer security problems and finally put an end to the cat-and-mouse game between attackers and defenders? Or is this hope merely hype? Now you can dive into the science and answer this question for yourself! With this practical guide, you'll explore ways to apply machine learning to security issues such as intrusion detection, malware classification, and network analysis. Machine learning and security specialists Clarence Chio and David Freeman provide a framework for discussing the marriage of these two fields, as well as a toolkit of machine-learning algorithms that you can apply to an array of security problems. This book is ideal for security engineers and data scientists alike. Learn how machine learning has contributed to the success of modern spam filters Quickly detect anomalies, including breaches, fraud, and impending system failure Conduct malware analysis by extracting useful information from computer binaries Uncover attackers within the network by finding patterns inside datasets Examine how attackers exploit consumer-facing websites and app functionality Translate your machine learning algorithms from the lab to production Understand the threat attackers pose to machine learning solutions

Biologically Inspired Design - Ashok K Goel 2013-07-16

From simple cases such as hook and latch attachments found in Velcro to articulated-wing flying vehicles, biology often has been used to inspire many creative design ideas. The scientific challenge now is to transform the paradigm into a repeatable and scalable methodology. Biologically Inspired Design explores computational techniques and tools that can help integrate the method into design practice. With an inspiring foreword from Janine Benyus, Biologically Inspired Design contains a dozen chapters written by some of the leading scholars in the transdisciplinary field of bioinspired design, such as Frank Fish, Julian Vincent and Jeannette Yen from biology, and Amaresk Chakrabarti, Satyandra Gupta and Li Shu from engineering. Based in part on discussions at two workshops sponsored by the United States National Science Foundation, this volume introduces and develops several methods and tools for bioinspired design including: Information-processing theories, Natural language techniques, Knowledge-based tools, and Functional approaches and Pedagogical techniques. By exploring these fundamental theories, techniques and tools for supporting biologically inspired design, this volume provides a comprehensive resource for design practitioners wishing to explore the paradigm, an invaluable guide to design educators interested in teaching the method, and a preliminary reading for design researchers wanting to investigate bioinspired design.

PC Hacks - Jim Aspinwall 2004-10-25

Intel-and AMD-powered PCs--which account for more than 90% of all personal computers--are powerful and expandable, and operating systems like Windows and Linux do a great job of running well on this hardware. But to maintain maximum stability and predictability, these operating systems don't push the hardware to its limits.That doesn't mean you can't.PC Hacks shows PC users like you how to get the most out of your hardware and software to make your PC experience more satisfying than ever. You don't need another collection of simple tips and command-clicks; you need PC Hacks, where you'll find proven techniques for enhancing performance and preventing problems with your PC hardware. This step-by-step, hack-by-hack guide, with invaluable tips and tricks throughout, will get you hacking the system board, CPU, BIOS, peripherals and operating system--everything but the unhackable power supply!In PC Hacks, Jim Aspinwall, the Windows Helpdesk columnist and feature editor for CNET.COM and author of three books on PC maintenance, delivers basic to advanced hacks for overclocking CPU and video cards, tweaking RAM timing, selecting the best performing components, and much more. He includes suggestions for reusing an old PC to off-load work from newer systems as well as ways to prevent security hacks. He also offers many tips for avoiding common mistakes--and for getting the system back up and running if something does go wrong.PC Hacks combines of the bestselling Hacks series style with the world's most popular computing hardware. Presented in a clear and direct format and covering both Windows and Linux operating systems, PC Hacks ensure that you'll hack and tweak your way to the best performance possible out of your trusty PC.

The New School of Information Security - Adam Shostack 2008-03-26

"It is about time that a book like The New School came along. The age of security as pure technology is long past, and modern practitioners need to understand the social and cognitive aspects of security if they are to be successful. Shostack and Stewart teach readers exactly what they need to know--I just wish I could have had it when I first started out." --David Mortman, CSO-in-Residence Echelon One, former CSO Siebel Systems Why is information security so dysfunctional? Are you wasting the money you spend on security? This book shows how to spend it more effectively. How can you make more effective security decisions? This book explains why professionals have taken to studying economics, not cryptography--and why you should, too. And why security breach notices are the best thing to ever happen to information security. It's about time someone asked the biggest, toughest questions about information security. Security experts Adam Shostack and Andrew Stewart don't just answer those questions--they offer honest, deeply troubling answers. They explain why these critical problems exist and how to solve them. Drawing on powerful lessons from economics and other disciplines, Shostack and Stewart offer a new way forward. In clear and engaging prose, they shed new light on the critical challenges that are faced by the security field. Whether you're a CIO, IT manager, or security specialist, this book will open your eyes to new ways of thinking about--and overcoming--your most pressing security challenges. The New School enables you to take control, while others struggle with non-stop crises. Better evidence for better decision-making Why the security data you have doesn't support effective decision-making--and what to do about it Beyond security "silos": getting the job done together Why it's so hard to improve security in isolation--and how the entire industry can make it happen and evolve Amateurs study cryptography; professionals study economics What IT security leaders can and must learn from other scientific fields A bigger bang for every buck How to re-allocate your scarce resources where they'll do the most good

Pig Design Patterns - Pradeep Pasupuleti 2014-04-17

A comprehensive practical guide that walks you through the multiple stages of data management in enterprise and gives you numerous design patterns with appropriate code examples to solve frequent problems in each of these stages. The chapters are organized to mimick the sequential data flow evidenced in Analytics platforms, but they can also be read independently to solve a particular group of problems in the Big Data life cycle. If you are an experienced developer who is already familiar with Pig and is looking for a use case standpoint where they can relate to the problems of data ingestion, profiling, cleansing, transforming, and egressing data encountered in the enterprises. Knowledge of Hadoop and Pig is necessary for readers to grasp the intricacies of Pig design patterns better.

Linux Network Administrator's Guide - Olaf Kirch 2000

This introduction to networking on Linux now covers firewalls, including the use of ipchains and Netfilter, masquerading, and accounting. Other new topics in this second edition include Novell (NCP/IPX) support and INN (news administration).

Professional JavaScript - Hugo Di Francesco 2019-09-30

Develop your JavaScript programming skills by learning strategies and techniques commonly used in modern full-stack application development Key FeaturesWrite and deploy full-stack applications efficiently with JavaScriptDelve into JavaScript’s multiple programming paradigmsGet up to speed with core concepts such as modularity and functional programming to write efficient codeBook Description In depth knowledge of JavaScript makes it easier to learn a variety of other frameworks, including React, Angular, and related tools and libraries. This book is designed to help you cover the core JavaScript concepts you need to build modern applications. You'll start by learning how to represent an HTML document in the Document Object Model (DOM). Then, you'll combine your knowledge of the DOM and Node.js to create a web scraper for practical situations. As you read through further lessons, you'll create a Node.js-based RESTful API using the Express library for Node.js. You'll also understand how modular designs can be used for better reusability and collaboration with multiple developers on a single project. Later lessons will guide you through building unit tests, which ensure that the core functionality of your program is not affected over time. The book will also demonstrate how constructors, async/await, and events can load your applications quickly and efficiently. Finally, you'll gain useful insights into functional programming concepts such as immutability, pure functions, and higher-order functions. By the end of this book, you'll have the skills you need to tackle any real-world JavaScript development problem using a modern JavaScript approach, both for the client and server sides. What you will learnApply the core concepts of functional programmingBuild a Node.js project that uses the Express.js library to host an APICreate unit tests for a Node.js project to validate itUse the Cheerio library with Node.js to create a basic web scraperDevelop a React interface to build processing flowsUse callbacks as a basic way to bring control backWho this book is for If you want to advance from being a frontend developer to a full-stack developer and learn how Node.js can be used for hosting full-stack applications, this is an ideal book for you. After reading this book, you'll be able to write better JavaScript code and learn about the latest trends in the language. To easily grasp the concepts explained here, you should know the basic syntax of JavaScript and should've worked with popular frontend libraries such as jQuery. You should have also used JavaScript with HTML and CSS but not necessarily Node.js.

Game Physics Cookbook - Gabor Szauer 2017-03-24

Discover over 100 easy-to-follow recipes to help you implement efficient game physics and collision detection in your games About This Book Get a comprehensive coverage of techniques to create high performance collision detection in games Learn the core mathematics concepts and physics involved in depicting collision detection for your games Get a hands-on experience of building a rigid body physics engine Who This Book Is For This book is for beginner to intermediate game developers. You don't need to have a formal education in games—you can be a hobbyist or indie developer who started making games with Unity 3D. What You Will Learn Implement fundamental maths so you can develop solid game physics Use matrices to encode linear transformations Know how to check geometric primitives for collisions Build a Physics engine that can create realistic rigid body behavior Understand advanced techniques, including the Separating Axis Theorem Create physically accurate collision reactions Explore spatial partitioning as an acceleration structure for collisions Resolve rigid body collisions between primitive shapes In Detail Physics is really important for game programmers who want to add realism and functionality to their games. Collision detection in particular is a problem that affects all game developers, regardless of the platform, engine, or toolkit they use. This book will teach you the concepts and formulas behind collision detection. You will also be taught how to build a simple physics engine, where Rigid Body physics is the main focus, and learn about intersection algorithms for primitive shapes. You'll begin by building a strong foundation in mathematics that will be used throughout the book. We'll guide you through implementing 2D and 3D primitives and show you how to perform effective collision tests for them. We then pivot to one of the harder areas of game development—collision detection and resolution. Further on, you will learn what a Physics engine is, how to set up a game window, and how to implement rendering. We'll explore advanced physics topics such as constraint solving. You'll also find out how to implement a rudimentary physics engine, which you can use to build an Angry Birds type of game or a more advanced game. By the end of the book, you will have implemented all primitive and some advanced collision tests, and you will be able to read on geometry and linear Algebra formulas to take forward to your own games! Style and approach Gain the necessary skills needed to build a Physics engine for your games through practical recipes, in an easy-to-read manner. Every topic explained in the book has clear, easy to understand code accompanying it.

The Million Word Crossword Dictionary - Stanley Newman 2010-11-09

With more than 1,300,000 answers, this volume contains more than twice as many words as any other crossword dictionary. Meticulously compiled by two crossword professionals with a combined fifty years in the field and based on a massive analysis of current crosswords, there has never been a crossword dictionary with the breadth, depth, and currency of this one. From Jim Carrey to Sister Carrie, Homer Simpson to Homer’s Iliad, the wide-ranging entries include 500,000+ synonyms, 3,000+ literary works, 3,000+ films, 20,000+ famous people from all fields, and more than 50,000 fill-in-the-blank clues so popular in today’s crosswords. Featuring an introduction by New York Times crossword editor Will Shortz, The Million Word Crossword Dictionary makes every other crossword dictionary obsolete. This edition offers thousands of new entries, including slang terms; brand names; celebrity names; and films, novelists’ works, sports Hall of Famers, automobile models, and more. The larger type size makes finding the answers easier than ever.

Big Data Security - Shibakali Gupta 2019-10-08

THE SERIES: FRONTIERS IN COMPUTATIONAL INTELLIGENCE The series Frontiers In Computational Intelligence is envisioned to provide comprehensive coverage and understanding of cutting edge research in computational intelligence. It intends to augment the scholarly discourse on all topics relating to the advances in artifi cial life and machine learning in the form of metaheuristics, approximate reasoning, and robotics. Latest research findings are coupled with applications to varied domains of engineering and computer sciences. This field is steadily growing especially with the advent of novel machine learning algorithms being applied to different domains of engineering and technology. The series brings together leading researchers that intend to continue to advance the field and create a broad knowledge about the most recent research. Series Editor Dr. Siddhartha Bhattacharyya, CHRIST (Deemed to be University), Bangalore, India Editorial Advisory Board Dr. Elizabeth Behrman, Wichita State University, Kansas, USA Dr. Goran Klepac Dr. Leo Mrsic, Algebra University College, Croatia Dr. Aboul Ella Hassanien, Cairo University, Egypt Dr. Jan Platos, VSB-Technical University of Ostrava, Czech Republic Dr. Xiao-Zhi Gao, University of Eastern Finland, Finland Dr. Wellington Pinheiro dos Santos, Federal University of Pernambuco, Brazil

Hands-On Artificial Intelligence for Cybersecurity - Alessandro Parisi 2019-08-02

Build smart cybersecurity systems with the power of machine learning and deep learning to protect your corporate assets Key FeaturesIdentify and predict security threats using artificial intelligenceDevelop intelligent systems that can detect unusual and suspicious patterns and attacksLearn how to test the effectiveness of your AI cybersecurity algorithms and toolsBook Description Today's organizations spend billions of dollars globally on cybersecurity. Artificial intelligence has emerged as a great solution for building smarter and safer security systems that allow you to predict and detect suspicious network activity, such as phishing or unauthorized intrusions. This cybersecurity book presents and demonstrates popular and successful AI approaches and models that you can adapt to detect potential attacks and protect your corporate systems. You'll learn about the role of machine learning and neural networks, as well as deep learning in cybersecurity, and you'll also learn how you can infuse AI capabilities into building smart defensive mechanisms. As you advance, you'll be able to apply these strategies across a variety of applications, including spam filters, network intrusion detection, botnet detection, and secure authentication. By the end of this book, you'll be ready to develop intelligent systems that can detect unusual and suspicious patterns and attacks, thereby developing strong network security defenses using AI. What you will learnDetect email threats such as spamming and phishing using AICategorize APT, zero-days, and polymorphic malware samplesOvercome antivirus limits in threat detectionPredict network intrusions and detect anomalies with machine learningVerify the strength of biometric authentication procedures with deep learningEvaluate cybersecurity strategies and learn how you can improve themWho this book is for If you’re a cybersecurity professional or ethical hacker who wants to build intelligent systems using the power of machine learning and AI, you’ll find this book useful. Familiarity with cybersecurity concepts and knowledge of Python programming is essential to get the most out of this book.

Exam Ref SC-900 Microsoft Security, Compliance, and Identity Fundamentals - Yuri Diogenes 2021-12-04

Prepare for Microsoft Exam SC-900 and help demonstrate your real-world knowledge of the fundamentals of security, compliance, and identity (SCI) across cloud-based and related Microsoft services. Designed for business stakeholders, new and existing IT professionals, functional consultants, and students, this Exam Ref focuses on the critical thinking and decision-making acumen needed for success at the Microsoft Certified: Security, Compliance, and Identity Fundamentals level. Focus on the expertise measured by these objectives: * Describe the concepts of security, compliance, and identity * Describe the capabilities of Microsoft identity and access management solutions * Describe the capabilities of Microsoft security solutions * Describe the capabilities of Microsoft compliance solutions This Microsoft Exam Ref: * Organizes its coverage by exam objectives * Features strategic, what-if scenarios to challenge you * Assumes you are a business user, stakeholder, consultant, professional, or student who wants to create holistic, end-to-end solutions with Microsoft security, compliance, and identity technologies About the Exam Exam SC-900 focuses on knowledge needed to describe: security and compliance concepts and methods; identity concepts; Azure AD identity services/types, authentication, access management, identity protection, and governance; Azure, Azure Sentinel, and Microsoft 365 security management; Microsoft 365 Defender threat protection and Intune endpoint security; Microsoft 365 compliance management, information protection, governance, insider risk, eDiscovery, and audit capabilities; and Azure resource governance. About Microsoft Certification Passing this exam fulfills your requirements for the Microsoft Certified: Security, Compliance, and Identity Fundamentals certification, helping to demonstrate your understanding of the fundamentals of security, compliance, and identity (SCI) across cloud-based and related Microsoft services. With this certification, you can move on to earn more advanced related Associate-level role-based certifications. See full details at: microsoft.com/learn