Ip Cameras Default Passwords Directory Ipvm

Sidestep VoIP Catastrophe the Foolproof Hacking Exposed Way "This book illuminates how remote users can probe, sniff, and modify your phones, phone switches, and networks that offer VoIP services. Most importantly, the authors offer solutions to mitigate the risk of deploying VoIP technologies." --Ron Gula, CTO of Tenable Network Security Block debilitating VoIP attacks by learning how to look at your network and devices through the eyes of the malicious intruder. Hacking Exposed VoIP shows you, step-by-step, how online criminals perform reconnaissance, gain access, steal data, and penetrate vulnerable systems. All hardware-specific and network-centered security issues are covered alongside detailed countermeasures, in-depth examples, and hands-on implementation techniques. Inside, you'll learn how to defend against the latest DoS, man-in-the-middle, call flooding, eavesdropping, VoIP fuzzing, signaling and audio manipulation, Voice SPAM/SPIT, and voice phishing attacks. Find out how hackers footprint, scan, enumerate, and pilfer VoIP networks and hardware Fortify Cisco, Avaya, and Asterisk systems Prevent DNS poisoning, DHCP exhaustion, and ARP table manipulation Thwart number harvesting, call pattern tracking, and conversation eavesdropping Measure and maintain VoIP network quality of service and VoIP conversation quality Stop DoS and packet flood-based attacks from disrupting SIP proxies and phones Counter REGISTER hijacking, INVITE flooding, and BYE call teardown attacks Avoid insertion/mixing of malicious audio Learn about voice SPAM/SPIT and how to prevent it Defend against voice phishing and identity theft scams

The business to business trade publication for information and physical Security professionals.

Passive and Active Measurement19th International Conference, PAM 2018, Berlin, Germany, March 26–27, 2018, ProceedingsSpringer

This reference text will benefit readers in enhancing their understanding of the recent technologies, protocols, and challenges in various stages of development of wireless communication and networking. The text discusses the cellular concepts of 4G, 5G, and 6G along with their challenges. It covers topics related to vehicular technology, wherein vehicles communicate with the traffic and the environment around them using short-range wireless signals. The text comprehensively covers important topics including use of the Internet of Things (IoT) in wireless communication, architecture, and protocols. It further covers the role of smart antennas in emerging wireless technologies. The book Discusses advanced techniques used in the field of wireless communication. Covers technologies including network slicing, 5G wireless communication, and TV white space technology. Discusses practical applications including drone delivery systems, public safety, IoT, virtual reality, and smart cities. Covers radio theory and applications for wireless communication with ranges of centimeters to hundreds of meters. Discusses important topics including metamaterials, inductance coupling for loop antennas, bluetooth low energy, wireless security, and wireless sensor networks. Discussing latest technologies including 5G, 6G, IoT, vehicular technology and TV white space technology, this text will be useful for senior undergraduate, graduate students, and professionals in the fields of electrical engineering, and electronics and communication engineering.

SEDA 2018

Defense against the Black Arts

A Roadmap for Building a Linux File and Print Server

Red Hat Linux Firewalls

Research Anthology on Business Continuity and Navigating Times of Crisis

Create Deep Learning and Reinforcement Learning apps for multiple platforms with TensorFlow Key Features Build TensorFlow-powered AI applications for mobile and embedded devices Learn modern AI topics such as computer vision, NLP, and deep

reinforcement learning Get practical insights and exclusive working code not available in the TensorFlow documentation Book Description As a developer, you always need to keep an eye out and be ready for what will be trending soon, while also focusing on what's trending currently. So, what's better than learning about the integration of the best of both worlds, the present and the future? Artificial Intelligence (AI) is widely regarded as the next big thing after mobile, and Google's TensorFlow is the leading open source machine learning framework, the hottest branch of AI. This book covers more than 10 complete iOS, Android, and Raspberry Pi apps powered by TensorFlow and built from scratch, running all kinds of cool TensorFlow models offline on-device: from computer vision, speech and language processing to generative adversarial networks and AlphaZero-like deep reinforcement learning. You'll learn how to use or retrain existing TensorFlow models, build your own models, and develop intelligent mobile apps running those TensorFlow models. You'll learn how to quickly build such apps with step-by-step tutorials and how to avoid many pitfalls in the process with lots of hard-earned troubleshooting tips. What you will learn Classify images with transfer learning Detect objects and their locations Transform pictures with amazing art styles Understand simple speech commands Describe images in natural language Recognize drawing with

Convolutional Neural Network and Long Short-Term Memory Predict stock price with Recurrent Neural Network in TensorFlow and Keras Generate and enhance images with generative adversarial networks Build AlphaZero-like mobile game app in TensorFlow and Keras Use TensorFlow Lite and Core ML on mobile Develop TensorFlow apps on Raspberry Pi that can move, see, listen, speak, and learn Who this book is for If you're an iOS/Android developer interested in building and retraining others' TensorFlow models and running them in your mobile apps, or if you're a TensorFlow developer and want to run your new and amazing TensorFlow models on mobile devices, this book is for you. You'll also benefit from this book if you're interested in TensorFlow Lite, Core ML, or TensorFlow on Raspberry Pi.

This book balances the behavioral and database aspects of customer relationship management, providing students with a comprehensive introduction to an often overlooked, but important aspect of marketing strategy. Baran and Galka deliver a book that helps students understand how an enhanced customer relationship strategy can differentiate an organization in a highly competitive marketplace. This edition has several new features: Updates that take into account the latest research and changes in organizational dynamics, business-to-business relationships, social media, database management, and technology advances that

impact CRM New material on big data and the use of mobile technology An overhaul of the social networking chapter, reflecting the true state of this dynamic aspect of customer relationship management today A broader discussion of the relationship between CRM and the marketing function, as well as its implications for the organization as a whole Cutting edge examples and images to keep readers engaged and interested A complete typology of marketing strategies to be used in the CRM strategy cycle: acquisition, retention, and win-back of customers With chapter summaries, key terms, questions, exercises, and cases, this book will truly appeal to upper-level students of customer relationship management. Online resources, including PowerPoint slides, an instructor's manual, and test bank, provide instructors with everything they need for a comprehensive course in customer relationship management.

This book constitutes the proceedings of the 19th International Conference on Passive and Active Measurement, PAM 2018, held in Berlin, Germany, in March 2018. The 20 full papers presented in this volume were carefully reviewed and selected from 50 submissions. The papers demonstrate the import and extent to which measurements pervade systems – from protocols to performance to security. They are organized in the following topical sections: models and inference; security and privacy; CDNs; DNS; certificates; interdomain routing; and analyzing protocols.

Today, cloud computing, big data, and the internet of things (IoT) are becoming indubitable parts of modern information and communication systems. They cover not only information and communication technology but also all types of systems in society including within the realms of business, finance, industry, manufacturing, and management. Therefore, it is critical to remain up-to-date on the latest advancements and applications, as well as current issues and challenges. The Handbook of Research on Cloud Computing and Big Data Applications in IoT is a pivotal reference source that provides relevant theoretical frameworks and the latest empirical research findings on principles, challenges, and applications of cloud computing, big data, and IoT. While highlighting topics such as fog computing, language interaction, and scheduling algorithms, this publication is ideally designed for software developers, computer engineers, scientists, professionals, academicians, researchers, and students.

GeoVision GV-VMS Quick Start Guide

Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions

Best Practices for Securing Infrastructure

Build 10+ Artificial Intelligence apps using TensorFlow Mobile and Lite for iOS, Android, and Raspberry Pi

Defend Your Base with Simple Circuits, Arduino, and Raspberry Pi

Kali Linux 2018: Assuring Security by

Penetration Testing

Develop foundational skills in ethical hacking and penetration testing while getting ready to pass the certification exam Key FeaturesLearn how to look at technology from the standpoint of an attackerUnderstand the methods that attackers use to infiltrate networksPrepare to take and pass the exam in one attempt with the help of hands-on examples and mock testsBook Description With cyber threats continually evolving, understanding the trends and using the tools deployed by attackers to determine vulnerabilities in your system can help secure your applications, networks, and devices. To outmatch attacks, developing an attacker's mindset is a necessary skill, which you can hone with the help of this cybersecurity book. This study guide takes a step-by-step approach to helping you cover all the exam objectives using plenty of examples and hands-on activities. You'll start by gaining insights into the different elements of InfoSec and a thorough understanding of ethical hacking terms and concepts. You'll then learn about various vectors, including network-based vectors, software-based vectors, mobile devices, wireless networks, and IoT devices. The book also explores attacks on emerging technologies such as the cloud, IoT, web apps, and servers and examines prominent tools and techniques used by hackers. Finally, you'll be ready to take mock tests, which will help you test your understanding of all the topics covered in the book. By the end of this book, you'll have obtained the

information necessary to take the 312-50 exam and become a CEH v11 certified ethical hacker. What you will learnGet to grips with information security and ethical hackingUndertake footprinting and reconnaissance to gain primary information about a potential targetPerform vulnerability analysis as a means of gaining visibility of known security weaknessesBecome familiar with the tools and techniques used by an attacker to hack into a target systemDiscover how network sniffing works and ways to keep your information secureExplore the social engineering techniques attackers use to compromise systemsWho this book is for This ethical hacking book is for security professionals, site admins, developers, auditors, security officers, analysts, security consultants, and network engineers. Basic networking knowledge (Network+) and at least two years of experience working within the InfoSec domain are expected.

Despite the increase of high-profile hacks, record-breaking data leaks, and ransomware attacks, many organizations don't have the budget to establish or outsource an information security (InfoSec) program, forcing them to learn on the job. For companies obliged to improvise, this pragmatic guide provides a security-101 handbook with steps, tools, processes, and ideas to help you drive maximum-security improvement at little or no cost. Each chapter in this book provides step-by-step instructions for dealing with a specific issue, including breaches and disasters, compliance,

network infrastructure and password management, vulnerability scanning, and penetration testing, among others. Network engineers, system administrators, and security professionals will learn tools and techniques to help improve security in sensible, manageable chunks. Learn fundamentals of starting or redesigning an InfoSec program Create a base set of policies, standards, and procedures Plan and design incident response, disaster recovery, compliance, and physical security Bolster Microsoft and Unix systems, network infrastructure, and password management Use segmentation practices and designs to compartmentalize your network Explore automated process and tools for vulnerability management Securely develop code to reduce exploitable errors Understand basic penetration testing concepts through purple teaming Delve into IDS, IPS, SOC, logging, and monitoring

A remote Maine island becomes the setting for a deadly game of cat-and-mouse in the Net Force novella KILL CHAIN. Natasha Mori and Bryan Ferrago work for the Net Force Cyber Squad, an elite government agency created to lead the charge against America's online enemies. They've traveled to Maine's coast for a project to study extreme weather forecasting—and hopefully enjoy a little vacation. But someone from Natasha's past has followed them and, as a hurricane approaches, sees a chance to take her out of commission permanently. A team of elite biotech-enhanced mercenaries has been assigned to eliminate her and any witnesses on

the island. Stranded in the storm of the century, cut off from all help, Natasha and Bryan must now find a way to escape her hunters—or become part of their murderous kill chain.

Publisher's Note: Products purchased from Third Party sellers are not guaranteed by the publisher for quality, authenticity, or access to any online entitlements included with the product. Essential Skills for a Successful IT Career Written by Mike Meyers, the leading expert on CompTIA certification and training, this up-to-date, full-color text will prepare you for the CompTIA Network+ exam N10-007 and help you become an expert networking technician. Fully revised for the latest CompTIA Network+ exam, including coverage of performance-based questions, the book contains helpful on-the-job tips, end-of-chapter practice questions, and hundreds of photographs and illustrations. Note: this textbook is intended for classroom use and answers to the end of chapter sections are only available to adopting instructors. Mike Meyers' CompTIA Network+ Guide to Managing and Troubleshooting Networks, Fifth Edition covers: • Network architectures • Cabling and topology • Ethernet basics • Network installation • TCP/IP applications and network protocols • Routing • Network naming • Advanced networking devices • IPv6 • Remote connectivity • Wireless networking • Virtualization and cloud computing • Mobile networking • Network operations • Managing risk • Network security • Network monitoring and

troubleshooting Online content includes: • 100+ practice exam questions in a customizable test engine • 20+ lab simulations to help you prepare for the performance-based questions • One hour of video training from Mike Meyers • Mike's favorite shareware and freeware networking tools and utilities Each chapter features: • Learning objectives • Photographs and illustrations • Real-world examples • Try This! and Cross Check exercises • Key terms highlighted • Tech Tips, Notes, and Warnings • Exam Tips • End-of-chapter quizzes and lab projects

Advancements and Challenges

IP Video Surveillance. An Essential Guide.

Net Force: Kill Chain

Security-Related Advanced Technologies in Critical Infrastructure Protection

Mac Life

Linux Transfer for Windows Network Admins

Master powerful techniques and approaches for securing IoT systems of all kinds–current and emerging Internet of Things (IoT) technology adoption is accelerating, but IoT presents complex new security challenges. Fortunately, IoT standards and standardized architectures are emerging to help technical professionals systematically harden their IoT environments. In Orchestrating and Automating Security for the Internet of Things, three Cisco experts show how to safeguard current and future IoT systems by delivering security through new NFV and SDN architectures and related IoT security standards. The authors first review the current state of IoT networks and architectures, identifying key security risks associated with nonstandardized early deployments and showing how early adopters have attempted to respond. Next, they introduce more mature architectures built around NFV and SDN. You'll discover why these lend themselves well to IoT and IoT security, and master advanced approaches for protecting them. Finally, the authors preview future approaches to improving IoT security and present real-world use case examples. This is an indispensable resource for all technical and security professionals, business security and risk managers, and consultants who are responsible for systems that incorporate or utilize IoT devices, or expect to be responsible for them. · Understand the challenges involved in securing current IoT networks and architectures · Master IoT security fundamentals, standards, and modern best practices · Systematically plan for IoT security · Leverage Software-Defined Networking (SDN) and Network Function Virtualization (NFV) to harden IoT networks · Deploy the advanced IoT platform, and use MANO to manage and orchestrate virtualized network functions · Implement platform security services including identity, authentication, authorization, and accounting · Detect threats and protect data in IoT environments · Secure IoT in the context of remote access and VPNs · Safeguard the IoT platform itself · Explore use cases ranging from smart cities and advanced energy systems to the connected car · Preview evolving concepts that will shape the future of IoT security

Drones are taking the world by storm. The technology and laws governing them change faster than we can keep up with. The Big Book of Drones covers everything from drone law to laws on privacy, discussing the history and evolution of drones to where we are today. If you are new to piloting, it also covers how to fly a drone including a pre-flight checklist. For those who are interested in taking drones to the next level, we discuss how to build your own using a 3D printer as well as many challenging projects for your drone. For the truly advanced, The Big Book of Drones discusses how to hack a drone. This includes how to perform a replay attack, denial of service attack, and how to detect a drone and take it down. Finally, the book also covers drone forensics. This is a new field of study, but one that is steadily growing and will be an essential area of inquiry as drones become more prevalent.

This book delves into how the Linux operating is constructed and how it works, all from the point of view of an administrator experienced both with computers in general and Windows architecture in particular. Then it covers the installation and configuration of a network file server, with user management as well as file and directory sharing. Finally, the book describes how to implement sample scenarios. This book shows the experienced Windows network administrator how to convert from a Windows-based server to a Linux based one.

Covers critical infrastructure protection, providing a rigorous treatment of risk, resilience, complex adaptive systems, and sector dependence Wide in scope, this classroom-tested book is the only one to emphasize a scientific approach to protecting the key infrastructures components of a nation. It analyzes the complex network of entities that make up a nation's infrastructure, and identifies vulnerabilities and risks in various sectors by combining network science, complexity theory, risk analysis, and modeling and simulation. This approach reduces the complex problem of protecting water supplies, energy pipelines, telecommunication stations, power grid, and Internet and Web networks to a much simpler problem of protecting a few critical nodes. The new third edition of Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation incorporates a broader selection of ideas and sectors than the previous book. Divided into three sections, the first part looks at the historical origins of homeland security and critical infrastructure, and emphasizes current policy. The second examines theory and foundations, highlighting risk and resilience in the context of complexity theory, network science, and the prevailing theories of catastrophe. The last part covers the individual sectors, including communications, internet, cyber threats, information technology, social networks, SCADA, water and water treatment, energy, and more. Covers theories of catastrophes, details of how sectors work, and how to deal with the problem of critical infrastructure protection’s enormity and complexity Places great emphasis on computer security and whole-community response Includes PowerPoint slides for use by lecturers, as well as an instructor's guide with answers to exercises Offers five robust appendices that augment the non-mathematical chapters with more rigorous explanations and mathematics Critical Infrastructure Protection in Homeland Security, Third Edition is an important book for upper-division undergraduates and first-year graduate students in political science, history, public administration, and computer technology. It will also be of great interest to professional security experts and policymakers.

Handbook of Research on Cloud Computing and Big Data Applications in IoT

Passive and Active Measurement

Full Circle Magazine #97

Theoretical and Practical Approach

The Big Book of Drones

Defensive Security Handbook

Conflict in cyberspace is becoming more prevalent in all public and private sectors and is of concern on many levels. As a result, knowledge of the topic is becoming essential across most disciplines. This book reviews and explains the technologies that underlie offensive and defensive cyber operations, which are practiced by a range of cyber actors including state actors, criminal enterprises, activists, and individuals. It explains the processes and technologies that enable the full spectrum of cyber operations. Readers will learn how to use basic tools for cyber security and pen-testing, and also be able to quantitatively assess cyber risk to systems and environments and discern and categorize malicious activity. The book provides key concepts of information age conflict technical basics/fundamentals needed to understand more specific remedies and activities associated with all aspects of cyber operations. It explains techniques associated with offensive cyber operations, with careful distinctions made between cyber ISR, cyber exploitation, and cyber attack. It explores defensive cyber operations and includes case studies that provide practical

information, making this book useful for both novice and advanced information warfare practitioners.

Where will you be when the zombie apocalypse hits? Trapping yourself in the basement? Roasting the family pet? Beheading reanimated neighbors? No way. You'll be building fortresses, setting traps, and hoarding supplies, because you, savvy survivor, have snatched up your copy of The Maker's Guide to the Zombie Apocalypse before it's too late. This indispensable guide to survival after Z-day, written by hardware hacker and zombie anthropologist Simon Monk, will teach you how to generate your own electricity, salvage parts, craft essential electronics, and out-survive the undead.,p>Take charge of your environment: –Monitor zombie movement with trip wires and motion sensors –Keep vigilant watch over your compound with Arduino and Raspberry Pi surveillance systems –Power zombie defense devices with car batteries, bicycle generators, and solar power Escape imminent danger: –Repurpose old disposable cameras for zombie-distracting flashbangs –Open doors remotely for a successful sprint home –Forestall subplot disasters with fire and smoke detectors Communicate with other survivors: –Hail nearby humans using Morse code –Pass silent messages with two-way vibration walkie-talkies –Fervently scan the airwaves with a frequency hopper For anyone from the budding maker to the keen hobbyist, The Maker's Guide to the Zombie Apocalypse is an essential survival tool. Uses the Arduino Uno board and Raspberry Pi Model B+ or Model 2

This 16th International Conference on Information Technology - New Generations (ITNG), continues an annual event focusing on state of the art technologies pertaining to digital information and communications. The applications of advanced information technology to such domains as astronomy, biology, education, geosciences, security and health care are among topics of relevance to ITNG. Visionary ideas, theoretical and experimental results, as well as prototypes, designs, and tools that help the information readily flow to the user are of special interest. Machine Learning, *Robotics, High Performance Computing, and Innovative Methods of Computing are examples of related topics. The conference features keynote speakers, the best student award, poster award, service award, a technical open panel, and workshops/exhibits from industry, government and academia.*

This book collects the latest research results on security-related advanced technologies. The chapters contain relevant and interesting topics from numerous research. Data science and artificial intelligence research nowadays one of the most important topics for the industry and the security sectors. The autonomy and counter-autonomy research topic are also very interesting. Autonomous cars have become a part of the common days, but their safe and secure application is not assured. The research results in this field want to support and assure safe and secure autonomous applications in our quotidian life. Also, the safe and secure robotics in the industries and the defence assure a high standard of living and the given research results in this area can use to increase it. The researchers work on it and publish the results that can be interesting for the other researchers and the innovators, but also the industrial part members. The researchers work on it and publish the results that can be interesting for the other researchers and the innovators, but also the industrial part members. Communication is a part of our life, but the communication systems mesh all around the world. Communication is the basis of modern life because without it life stop. One other interesting and very important research area is the material sciences. Virtual life cannot exist without hardware and materials. The new technical applications require new materials, that can suffice the mechanical and physical, chemical properties demand. Nowadays a common requirement of the materials the high strength and lightweight. Researchers want to serve the industrial requests and innovate new composite materials or increase the properties of the material through a new technological process. The authors publish the latest results of the security-

related research area including the newest innovations and technologies which rise the interest of the defence and the modern industries even the interest of other researchers.

Keep up to date with ethical hacking trends and hone your skills with hands-on activities

The Maker's Guide to the Zombie Apocalypse

Digital Video Surveillance and Security

Mastering Red Hat Linux 9

Mike Meyers CompTIA Network Guide to Managing and Troubleshooting Networks Fifth Edition (Exam N10-007)

Delivering Advanced Security Capabilities from Edge to Cloud for IoT

This book provides solid, state-of-the-art contributions from both scientists and practitioners working on botnet detection and analysis, including botnet economics. It presents original theoretical and empirical chapters dealing with both offensive and defensive aspects in this field. Chapters address fundamental theory, current trends and techniques for evading detection, as well as practical experiences concerning detection and defensive strategies for the botnet ecosystem, and include surveys, simulations, practical results, and case studies.

This book constitutes the refereed proceedings of the First Conference on Cybersecurity of Industrial Control Systems, CyberICS 2015, and the First Workshop on the Security of Cyber Physical Systems, WOS-CPS 2015, held in Vienna, Austria, in September 2015 in conjunction with ESORICS 2015, the 20th annual European Symposium on Research in Computer Security. The 6 revised full papers and 2 short papers of CyberICS 2015 presented together with 3 revised full papers of WOS-CPS 2015 were carefully reviewed and selected from 28 initial submissions. CyberICS 2015 focuses on topics covering ICSs, including cyber protection and cyber defense of SCADA systems, plant control systems, engineering workstations, substation equipment, programmable logic controllers, PLCs, and other industrial control system. WOS-CPS 2015 deals with the Security of Cyber Physical Systems, that exist everywhere around us, and range in size, complexity and criticality, from embedded systems used in smart vehicles, to SCADA systems in smart grids to control systems in water distribution systems, to smart transportation systems etc.

The use of digital surveillance technology is rapidly growing as it becomes significantly cheaper for live and remote monitoring. The second edition of Digital Video Surveillance and Security provides the most current and complete reference for security professionals and consultants as they plan, design, and implement surveillance systems to secure their places of business. By providing the necessary explanations of terms, concepts, and technological capabilities, this revised edition addresses the newest technologies and solutions available on the market today. With clear descriptions and detailed illustrations, Digital Video Surveillance and Security is the only book that shows the need for an overall understanding of the digital video surveillance (DVS) ecosystem. Highly visual with easy-to-read diagrams, schematics, tables, troubleshooting charts, and graphs Includes design and implementation case studies and best practices Uses vendor-neutral comparisons of the latest camera equipment and recording options

When the COVID-19 pandemic caused a halt in global society, many business leaders found themselves unprepared for the unprecedented change that swept across industry. Whether the need to shift to remote work or the inability to safely conduct business during a global pandemic, many businesses struggled in the transition to the “new normal.” In the wake of the pandemic, these struggles have created opportunities to study how businesses navigate these times of crisis. The Research Anthology on Business Continuity and Navigating Times of Crisis discusses the strategies, cases, and research surrounding business continuity throughout crises such as pandemics. This book analyzes business operations and the state of the economy during times of crisis and the leadership involved in recovery. Covering topics such as crisis management, entrepreneurship, and business sustainability, this four-volume comprehensive major reference work is a valuable resource for managers, CEOs, business leaders, entrepreneurs, professors and students of higher education, researchers, and academicians.

Ethical Hacking and Countermeasures: Attack Phases

THE INDEPENDENT MAGAZINE FOR THE UBUNTU LINUX COMMUNITY

How Hackers Do What They Do and How to Protect against It

Managing IoT Systems for Institutions and Cities

Defending a Networked Nation

Botnets

MacLife is the ultimate magazine about all things Apple. It’s authoritative, ahead of the curve and endlessly entertaining. MacLife provides unique content that helps readers use their Macs, iPhones, iPods, and their related hardware and software in every facet of their personal and professional lives.

This book gathers selected research papers presented at the Third International Conference on Communication and Intelligent Systems (ICCIS 2021), organized by National institute of Technology, Delhi, India, during December 18–19, 2021. This book presents a collection of state-of-the-art research work involving cutting-edge technologies for communication and intelligent systems. Over

the past few years, advances in artificial intelligence and machine learning have sparked new research efforts around the globe, which explore novel ways of developing intelligent systems and smart communication technologies. The book presents single- and multi-disciplinary research on these themes in order to make the latest results available in a single, readily accessible source.
Achieve the gold standard in penetration testing with Kali using this masterpiece, now in its fourth edition Key FeaturesRely on the most updated version of Kali to formulate your pentesting strategiesTest your corporate network against threatsExplore new cutting-edge wireless penetration tools and featuresBook Description Kali Linux is a comprehensive penetration testing platform with advanced tools to identify, detect, and exploit the vulnerabilities uncovered in the target network environment. With Kali Linux, you can apply the appropriate testing methodology with defined business objectives and a scheduled test plan, resulting in successful penetration testing project engagement. This fourth edition of Kali Linux 2018: Assuring Security by Penetration Testing starts with the installation of Kali Linux. You will be able to create a full test environment to safely practice scanning, vulnerability assessment, and exploitation. You’ll explore the essentials of penetration testing by collecting relevant data on the target network with the use of several

footprinting and discovery tools. As you make your way through the chapters, you'll focus on specific hosts and services via scanning and run vulnerability scans to discover various risks and threats within the target, which can then be exploited. In the concluding chapters, you'll apply techniques to exploit target systems in order to gain access and find a way to maintain that access. You'll also discover techniques and tools for assessing and attacking devices that are not physically connected to the network, including wireless networks. By the end of this book, you will be able to use NetHunter, the mobile version of Kali Linux, and write a detailed report based on your findings. What you will learnConduct the initial stages of a penetration test and understand its scopePerform reconnaissance and enumeration of target networksObtain and crack passwordsUse Kali Linux NetHunter to conduct wireless penetration testingCreate proper penetration testing reportsUnderstand the PCI-DSS framework and tools used to carry out segmentation scans and penetration testingCarry out wireless auditing assessments and penetration testingUnderstand how a social engineering attack such as phishing worksWho this book is for This fourth edition of Kali Linux 2018: Assuring Security by Penetration Testing is for pentesters, ethical hackers, and IT security professionals with basic knowledge of Unix/Linux operating systems. Prior knowledge of information security will help you understand the concepts in this book

Learn how to build your own computer vision (CV) applications quickly and easily with SimpleCV, an open source framework written in Python. Through examples of real-world applications, this hands-on guide introduces you to basic CV techniques for collecting, processing, and analyzing streaming digital images. You'll then learn how to apply these methods with SimpleCV, using sample Python code. All you need to get started is a Windows, Mac, or Linux system, and a willingness to put CV to work in a variety of ways. Programming experience is optional. Capture images from several sources, including webcams, smartphones, and Kinect Filter image input so your application processes only necessary information Manipulate images by performing basic arithmetic on pixel values Use feature detection techniques to focus on interesting parts of an image Work with several features in a single image, using the NumPy and SciPy Python libraries Learn about optical flow to identify objects that change between two image frames Use SimpleCV's command line and code editor to run examples and test techniques

Cyberwarfare: An Introduction to Information-Age Conflict

Unleash the full potential of Kali Linux 2018, now with updated tools, 4th Edition

Architectures, Countermeasures, and

Challenges

Intelligent Mobile Projects with TensorFlow

Certified Ethical Hacker (CEH) v11 312-50 Exam Guide

Critical Infrastructure Protection in Homeland Security

Migrate to Intent-Based Networking–and improve network manageability, cost, agility, security, and simplicity With Intent-Based Networking (IBN), you can create networks that capture and automatically activate business intent, assure that your network responds properly, proactively detect and contain security threats, and remedy network issues before users even notice. Intent-Based Networking makes networks far more valuable, but few organizations have the luxury of building them from the ground up. In this book, leading expert Pieter-Jans Nefkens presents a unique four-phase approach to preparing and transforming campus network infrastructures, architectures, and organization–helping you gain maximum value from IBN with minimum disruption and cost. The author reviews the problems IBN is intended to solve, and illuminates its technical, business, and cultural implications. Drawing on his pioneering experience, he makes specific recommendations, identifies pitfalls, and shows how to overcome them. You'll learn how to implement IBN with the Cisco Digital Network Architecture and DNA Center and walk through real-world use cases. In a practical *appendix, Nefkens even offers detailed technical configurations to jumpstart your own transformation. Review classic campus network deployments and understand why they need to change Learn how Cisco Digital Network Architecture (DNA) provides a solid foundation for state-of-the-art next generation network infrastructures Understand "intent" and how it can be applied to network infrastructure Explore tools for enabling, automating, and assuring Intent-Based Networking within campus networks Transform to Intent-Based Networking using a four-phased approach: Identify challenges; Prepare for Intent; Design and Deploy; and Enable Intent Anticipate how Intent-Based Networking will change your enterprise architecture, IT operations, and business*

** Everything readers need to construct firewalls that protect computer networks from attacks and intrusions * Covers the migration from ipchains and how to mange iptable log files * Reviews the customization of firewalls, the Red Hat firewall tool, the firewall setup, and advanced firewall features * Includes numerous examples of firewalls and firewall administration techniques that work on Red Hat Linux systems * Explains how to cost-justify, implement, test, and operate packet filtering firewalls constructed using Red Hat Linux RED HAT(r) PRESS(TM) Linux Solutions from the Experts at Red Hat Red Hat-the world's leading Linux company-presents a series of unrivaled guides* *that are reviewed and approved by the experts at Red Hat. Each book is packed with invaluable tips and techniques that are ideal for everyone from beginning to advanced network and systems professionals, as well as home and small businesses.*

This new edition discusses IP address management (IPAM) needs and methods that have evolved over the past decade. Such evolution includes mainstream use of private and public cloud services, maturation of IPv6 implementations, increased interest in DNS security approaches, and proliferation of Internet of Things (IoT) devices. These broad trends are serving to broaden the IPAM purview of network managers. The book begins with a basic overview of IP networking, including a discussion of protocol layering, addressing, and routing. After a review of the IP address management (IPAM) technologies, the book introduces the major components, motivation, benefits, and basic approaches of IPAM.

Your Complete Guide to the World's Leading Linux Distribution Whether you depend on Linux as a server or desktop OS, Mastering Red Hat Linux 9 gives you the practical information you need to install, configure, and administer the latest version of Red Hat's operating system to suit your specific computing needs. Clear, step-by-step instruction teaches you basic, intermediate, and advanced techniques, and the Publisher's Edition of Red Hat Linux 9—included on two

CDs—lets you get started right away. Coverage includes: Installing Linux from multiple sources Automating Linux installation over a network Navigating the command line interface Administering users and groups Managing RPM packages Troubleshooting the boot process Recompiling a kernel Configuring the X Window Working with GNOME and KDE Using Red Hat GUI administrative tools Understanding basic TCP/IP networking Securing Linux firewalls Setting up secure remote access Installing and testing DNS, DHCP, CUPS, and sendmail Configuring and troubleshooting FTP, NFS, Samba, and Apache Online Bonus Chapters: Linux Certification requirments (not yet available) Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

Security of Industrial Control Systems and Cyber Physical Systems

The Foundation of Contemporary Marketing Strategy

Wireless Communication

Customer Relationship Management

Practical Computer Vision with SimpleCV

First Workshop, CyberICS 2015 and First Workshop, WOS-CPS 2015 Vienna, Austria, September 21-22, 2015 Revised Selected Papers

In an effort to get her security consulting business off the ground, Kelsey Allen has been spending a lot of time up in the air, rappelling down buildings and climbing through windows to show business owners their vulnerabilities to thieves. When she is hired to pose as a conservator at the Pink Palace Museum in order to test their security weaknesses after some artifacts go missing, she's ecstatic. But when her investigative focus turns from theft to murder, Kelsey knows she's out of her league--and possibly in the cross hairs. When blast-from-the-past Detective Brad Hollister is called in to investigate, Kelsey may find that he's the biggest security threat yet . . . to her heart. Crackling with romantic tension and laced with intrigue, this suspenseful story from award-winning author Patricia Bradley will keep readers guessing--and looking over their shoulders.

The EC-Council | Press Ethical Hacking and Countermeasures Series is comprised of five books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack and secure information systems. With the full series of books, the reader will gain in-depth knowledge and practical experience with essential security systems, and become prepared to succeed on the Certified Ethical Hacker, or C|EH, certification from EC-Council. This certification covers a plethora of offensive security topics ranging from how perimeter defenses work, to scanning and attacking simulated networks. A wide variety of tools, viruses, and malware is presented in this and the other four books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, an Ethical Hacker will be able to set up strong countermeasures and defensive systems to protect an organization's critical infrastructure and information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This book defines what IoT Systems manageability looks like and what the associated resources and costs are of that manageability. It identifies IoT Systems performance expectations and addresses the difficult challenges of determining actual costs of IoT Systems implementation, operation, and management across multiple institutional organizations. It details the unique challenges that cities and institutions have in implementing and operating IoT Systems.

As technology has developed, computer hackers have become increasingly sophisticated, mastering the ability to hack into even the most impenetrable systems. The best way to secure a system is to understand the tools hackers use and know how to circumvent them. Defense against the Black Arts: How Hackers Do What They Do and How to Protect against It provides hands-on instruction to a host of techniques used to hack into a variety of systems. Exposing hacker methodology with concrete examples, this book shows you how to outwit computer predators at their own game. Among the many things you'll learn: How to get into a Windows operating system without having the username or password Vulnerabilities associated with passwords and how to keep them out of the hands of hackers How hackers use the techniques of computer forensic examiners to wreak havoc on individuals and companies Hiding one's IP address to avoid detection Manipulating data to and from a web page or application for nefarious reasons How to find virtually anything on the internet How hackers research the targets they plan to attack How network defenders collect traffic across the wire to indentify intrusions Using Metasploit to attack weaknesses in systems that are unpatched or have poorly implemented security measures The book profiles a variety of attack tools and examines how Facebook and other sites can be used to conduct social networking attacks. It also covers techniques utilized by hackers to attack modern operating systems, such as Windows 7, Windows Vista, and Mac OS X. The author explores a number of techniques that hackers can use to exploit physical access, network access, and wireless vectors. Using screenshots to clarify procedures, this practical manual uses step-by-step examples and relevant analogies to facilitate understanding, giving you an insider's view of the secrets of hackers.

Hacking Multifactor Authentication
Orchestrating and Automating Security for the Internet of Things
16th International Conference on Information Technology-New Generations (ITNG 2019)
19th International Conference, PAM 2018, Berlin, Germany, March 26–27, 2018, Proceedings
Transforming Campus Networks to Intent-Based Networking
IP Address Management

This month: * Command & Conquer * How-To : Run Android Apps in Ubuntu, LibreOffice, Using LaTeX, and Programming JavaScript * Graphics : Inkscape.* Chrome Cult * Linux Labs: IP Camera with Powerline Adapter* Ubuntu Phones * Review: KDE Plasma 5* Ubuntu Games: This War of Mineplus: News, Arduino, Q&A, and soooo much more.

This book presents high-quality original contributions on new software engineering models, approaches, methods, and tools and their evaluation in the context of defence and security applications. In addition, important business and economic aspects are discussed, with a particular focus on cost/benefit analysis, new business models, organizational evolution, and

business intelligence systems. The contents are based on presentations delivered at SEDA 2018, the 6th International Conference in Software Engineering for Defence Applications, which was held in Rome, Italy, in June 2018. This conference series represents a targeted response to the growing need for research that reports and debates the practical implications of software engineering within the defence environment and also for software performance evaluation in real settings through controlled experiments as well as case and field studies. The book will appeal to all with an interest in modeling, managing, and implementing defence-related software development products and processes in a structured and supportable way.

Protect your organization from scandalously easy-to-hack MFA security "solutions" Multi-Factor Authentication (MFA) is spreading like wildfire across digital environments. However, hundreds of millions of dollars have been stolen from MFA-protected online accounts. How? Most people who use multifactor authentication (MFA) have been told *that it is far less hackable than other types of authentication, or even that it is unhackable. You might be shocked to learn that all MFA solutions are actually easy to hack. That’s right: there is no perfectly safe MFA solution. In fact, most can be hacked at least five different ways. Hacking Multifactor Authentication will show you how MFA works behind the scenes and how poorly linked multi-step authentication steps allows MFA to be hacked and compromised. This book covers over two dozen ways that various MFA solutions can be hacked, including the methods (and defenses) common to all MFA solutions. You’ll learn about the various types of MFA solutions, their strengthens and weaknesses, and how to pick the best, most defensible MFA solution for your (or your customers') needs. Finally, this book reveals a simple method for quickly evaluating your existing MFA solutions. If using or developing a secure MFA solution is important to you, you need this book. Learn how different types of multifactor authentication work behind the scenes See how easy it is to hack*

MFA security solutions—no matter how secure they seem Identify the strengths and weaknesses in your (or your customers') existing MFA security and how to mitigate Author Roger Grimes is an internationally known security expert whose work on hacking MFA has generated significant buzz in the security world. Read this book to learn what decisions and preparations your organization needs to take to prevent losses from MFA hacking.

Proceedings of 6th International Conference in Software Engineering for Defence Applications

Communication and Intelligent Systems

Justice Buried (Book #2)

CSO

Proceedings of ICCIS 2021