Certified Scada Security Architect Cssa Iacertification

Hacking Connected Cars
The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601)
CYBERSECURITY- CAREER PATHS AND PROGRESSION
IT-Sicherheit in Industrie 4.0
Kali Linux Network Scanning Cookbook
CEH v9
Hands on Hacking
Linux in a Nutshell
Refactoring for Software Design Smells
Industrial Controls Security
The Smartest Person in the Room
Labor Impacts
Managing Cybersecurity in the Process Industries
The Measurement and Analysis of Housing Preference and Choice
Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions
UNIX Systems Programming for SVR4
IT Certification Success Exam Cram 2
Cybercrime Investigations
Security Metrics
Proceedings of the 16th International Conference on Cyber Warfare and Security-ICCWS 2021
Industrial Cybersecurity
Twelve Years a Slave
Cyber-security of SCADA and Other Industrial Control Systems
Kali Linux Cookbook
The PayPal Wars
An Introduction to Cyber Security
Cybersecurity in Our Digital Lives
Computer Security
Applied Cyber Security and the Smart Grid
El libro del Hacker. Edición 2022
Power Control Electronics
16th International Conference on Cyber Warfare and Security
Digital Forensics and Incident Response
Industrial Network Security
Cyber Crisis
Comptia Linux+ Xk0-004 Cert Guide
Cybersecurity for the Home and Office
Automating Manufacturing Systems with Plcs

SHEPPARD CHURCH

Hacking Connected Cars Packt Publishing Ltd
Over the last few years, Linux has grown both as an operating system and a tool for personal and business use. Simultaneously becoming more user friendly and more powerful as a back-end system, Linux has achieved new plateaus: the newer filesystems have solidified, new commands and tools have appeared and become standard, and the desktop--including new desktop environments--have proved to be viable, stable, and readily accessible to even those who don't consider themselves computer gurus. Whether you're using Linux for personal software projects, for a small office or home office (often termed the SOHO environment), to provide services to a small group of colleagues, or to administer a site responsible for millions of email and web connections each day, you need quick access to information on a wide range of tools. This book covers all aspects of administering and making effective use of Linux systems. Among its topics are booting, package management, and revision control. But foremost in Linux in a Nutshell are the utilities and commands that make Linux one of the most powerful and flexible systems available. Now in its fifth edition, Linux in a Nutshell brings users up-to-date with the current state of Linux. Considered by many to be the most complete and authoritative command reference for Linux available, the book covers all substantial user, programming, administration, and networking commands for the most common Linux distributions. Comprehensive but concise, the fifth edition has been updated to cover new features of major Linux distributions. Configuration information for the rapidly growing commercial network services and community update services is one of the subjects covered for the first time. But that's just the beginning. The book covers editors, shells, and LILO and GRUB boot options. There's also coverage of Apache, Samba, Postfix, sendmail, CVS, Subversion, Emacs, vi, sed, gawk, and much more. Everything that system administrators, developers, and power users need to know about Linux is referenced here, and they will turn to this book again and again.

The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601) Oreilly & Associates Incorporated
Awareness of design smells – indicators of common design problems – helps developers or software engineers understand mistakes made while designing, what design principles were overlooked or misapplied, and what principles need to be applied properly to address those smells through refactoring. Developers and software engineers may "know" principles and patterns, but are not aware of the "smells" that exist in their design because of wrong or mis-application of principles or patterns. These smells tend to contribute heavily to technical debt – further time owed to fix projects thought to be complete – and need to be addressed via proper refactoring. Refactoring for Software Design Smells presents 25 structural design smells, their role in identifying design issues, and potential refactoring solutions. Organized across common areas of software design, each smell is presented with diagrams and examples illustrating the poor design practices and the problems that result, creating a catalog of nuggets of readily usable information that developers or engineers can apply in their projects. The authors distill their research and experience as consultants and trainers, providing insights that have been used to improve refactoring and reduce the time and costs of managing software projects. Along the way they recount anecdotes from actual projects on which the relevant smell helped address a design issue. Contains a comprehensive catalog of 25 structural design smells (organized around four fundamental design principles) that contribute to technical debt in software projects Presents a unique naming scheme for smells that helps understand the cause of a smell as well as points toward its potential refactoring Includes illustrative examples that showcase the poor design practices underlying a smell and the problems that result Covers pragmatic techniques for refactoring design smells to manage technical debt and to create and maintain high-quality software in practice Presents insightful anecdotes and case studies drawn from the trenches of real-world projects
CYBERSECURITY- CAREER PATHS AND PROGRESSION Springer
A practical guide to deploying digital forensic techniques in response to cyber security incidents About This Book Learn incident response fundamentals and create an effective incident response framework Master forensics investigation utilizing digital investigative techniques Contains real-life scenarios that effectively use threat intelligence and modeling techniques Who This Book Is For This book is targeted at Information Security professionals, forensics practitioners, and students with knowledge and experience in the use of software applications and basic command-line experience. It will also help professionals who are new to the incident response/digital forensics role within their organization. What You Will Learn Create and deploy incident response capabilities within your organization Build a solid foundation for acquiring and handling suitable evidence for later analysis Analyze collected evidence and determine the root cause of a security incident Learn to integrate digital forensic techniques and procedures into the overall incident response process Integrate threat intelligence in digital evidence analysis Prepare written documentation for use internally or with external parties such as regulators or law enforcement agencies In Detail Digital Forensics and Incident Response will guide you through the entire spectrum of tasks associated with incident response, starting with preparatory activities associated with creating an incident response plan and creating a digital forensics capability within your own organization. You will then begin a detailed examination of digital forensic techniques including acquiring evidence, examining volatile memory, hard drive assessment, and network-based evidence. You will also explore the role that threat intelligence plays in the incident response process. Finally, a detailed section on preparing reports will help you prepare a written report for use either internally or in a courtroom. By the end of the book, you will have mastered forensic techniques and incident response and you will have a solid foundation on which to increase your ability to investigate such incidents in your organization. Style and approach The book covers practical scenarios and examples in an enterprise setting to give you an understanding of how digital forensics integrates with the overall response to cyber security incidents. You will also learn the proper use of tools and techniques to investigate common cyber security incidents such as malware infestation, memory analysis, disk analysis, and network analysis.
IT-Sicherheit in Industrie 4.0 Applied Cyber Security and the

Smart Grid
This book provides a comprehensive overview of the fundamental security of Industrial Control Systems (ICSs), including Supervisory Control and Data Acquisition (SCADA) systems and touching on cyber-physical systems in general. Careful attention is given to providing the reader with clear and comprehensive background and reference material for each topic pertinent to ICS security. This book offers answers to such questions as: Which specific operating and security issues may lead to a loss of efficiency and operation? What methods can be used to monitor and protect my system? How can I design my system to reduce threats?This book offers chapters on ICS cyber threats, attacks, metrics, risk, situational awareness, intrusion detection, and security testing, providing an advantageous reference set for current system owners who wish to securely configure and operate their ICSs. This book is appropriate for non-specialists as well. Tutorial information is provided in two initial chapters and in the beginnings of other chapters as needed. The book concludes with advanced topics on ICS governance, responses to attacks on ICS, and future security of the Internet of Things.
Kali Linux Network Scanning Cookbook Syngress
A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking techniques to better understand real-world risks to computer networks and data. Readers will benefit from the author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker’s perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you’ll look for flaws and their known exploits—including tools developed by real-world government financed state-actors. An introduction to the same hacking techniques that malicious hackers will use against an organization Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws Based on the tried and tested material used to train hackers all over the world in the art of breaching networks Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won't find any hypothetical academic only attacks here. From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to advanced techniques in a structured learning format.
CEH v9 BecomeShakespeare.com
Based on news reports, you might think there's a major cybersecurity threat every four to five months. In reality, there's a cybersecurity attack happening every minute of every day. Today, we live our lives—and conduct our business—online. Our data is in the cloud and in our pockets on our smartphones, shuttled over public Wi-Fi and company networks. To keep it safe, we rely on passwords and encryption and private servers, IT departments and best practices. But as you read this, there is a 70 percent chance that your data is compromised . . . you just don't know it yet. Cybersecurity attacks have increased exponentially, but because they're stealthy and often invisible, many underplay, ignore, or simply don't realize the danger. By the time they discover a breach, most individuals and businesses have been compromised for over three years. Instead of waiting until a problem surfaces, avoiding a data disaster means acting now to prevent one. In Cyber Crisis, Eric Cole gives readers a clear-eyed picture of the information war raging in cyberspace. Drawing on 30 years of experience—as a professional hacker for the CIA, as the Obama administration's cybersecurity commissioner, and as a consultant to clients around the globe from Bill Gates to Lockheed Martin and McAfee—Cole offers practical, actionable advice that even those with little technical background can implement, including steps to take on a daily, weekly, and monthly basis to protect their businesses and themselves. No matter who you are or where you work, cybersecurity should be a top priority. The information infrastructure we rely on in every sector of our lives—in healthcare and finance, for governments and private citizens—is both critical and vulnerable, and sooner or later, you or your company will be a target. This book is your guide to understanding the threat and putting together a proactive plan to minimize exposure and damage, and ensure the security of your business, your family, and your future
Hands on Hacking Morgan Kaufmann
As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems—energy production, water, gas, and other vital systems—becomes more important, and heavily mandated. Industrial Network Security, Second Edition arms you with the knowledge you need to understand the vulnerabilities of these distributed supervisory and control systems. The book examines the unique protocols and applications that are the foundation of industrial control systems, and provides clear guidelines for their protection. This how-to guide gives you thorough understanding of the unique challenges facing critical infrastructures, new guidelines and security measures for critical infrastructure protection, knowledge of new and evolving security tools, and pointers on SCADA protocols and security implementation. All-new real-world examples of attacks against control systems, and more diagrams of systems Expanded coverage of protocols such as 61850, Ethernet/IP, CIP, ISA-99, and the evolution to IEC62443 Expanded coverage of Smart Grid security New coverage of signature-based detection, exploit-based vs. vulnerability-based detection, and signature reverse engineering
Linux in a Nutshell Packt Publishing Ltd
"Having been born a freeman, and for more than thirty years enjoyed the blessings of liberty in a free State—and having at the end of that time been kidnapped and sold into Slavery, where I remained, until happily rescued in the month of January, 1853, after a bondage of twelve years—it has been suggested that an account of my life and fortunes would not be uninteresting to the public." -an excerpt
Refactoring for Software Design Smells Kohlhammer Verlag
Provides the nitty gritty details on how UNIX interacts with applications. Inlcudes many extended examples on topics ranging from string manipulation to network programming
Industrial Controls Security Certification Guide

What are the current trends in housing? Is my planned project commercially viable? What should be my marketing and advertisement strategies? These are just some of the questions real estate agents, landlords and developers ask researchers to answer. But to find the answers, researchers are faced with a wide variety of methods that measure housing preferences and choices. To select and value a valid research method, one needs a well-structured overview of the methods that are used in housing preference and housing choice research. This comprehensive introduction to this field offers just such an overview. It discusses and compares numerous methods, detailing the potential limitation of each one, and it reaches beyond methodology, illustrating how thoughtful consideration of methods and techniques in research can help researchers and other professionals to deliver products and services that are more in line with residents' needs.

The Smartest Person in the Room BenBella Books

Learn to defend crucial ICS/SCADA infrastructure from devastating attacks the tried-and-true Hacking Exposed way This practical guide reveals the powerful weapons and devious methods cyber-terrorists use to compromise the devices, applications, and systems vital to oil and gas pipelines, electrical grids, and nuclear refineries. Written in the battle-tested Hacking Exposed style, the book arms you with the skills and tools necessary to defend against attacks that are debilitating—and potentially deadly. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions explains vulnerabilities and attack vectors specific to ICS/SCADA protocols, applications, hardware, servers, and workstations. You will learn how hackers and malware, such as the infamous Stuxnet worm, can exploit them and disrupt critical processes, compromise safety, and bring production to a halt. The authors fully explain defense strategies and offer ready-to-deploy countermeasures. Each chapter features a real-world case study as well as notes, tips, and cautions. Features examples, code samples, and screenshots of ICS/SCADA-specific attacks Offers step-by-step vulnerability assessment and penetration test instruction Written by a team of ICS/SCADA security experts and edited by Hacking Exposed veteran Joel Scambray

Labor Impacts CRC Press

The Definitive Guide to Quantifying, Classifying, and Measuring Enterprise IT Security Operations Security Metrics is the first comprehensive best-practice guide to defining, creating, and utilizing security metrics in the enterprise. Using sample charts, graphics, case studies, and war stories, Yankee Group Security Expert Andrew Jaquith demonstrates exactly how to establish effective metrics based on your organization's unique requirements. You'll discover how to quantify hard-to-measure security activities, compile and analyze all relevant data, identify strengths and weaknesses, set cost-effective priorities for improvement, and craft compelling messages for senior management. Security Metrics successfully bridges management's quantitative viewpoint with the nuts-and-bolts approach typically taken by security professionals. It brings together expert solutions drawn from Jaquith's extensive consulting work in the software, aerospace, and financial services industries, including new metrics presented nowhere else. You'll learn how to: • Replace nonstop crisis response with a systematic approach to security improvement • Understand the differences between "good" and "bad" metrics • Measure coverage and control, vulnerability management, password quality, patch latency, benchmark scoring, and business-adjusted risk • Quantify the effectiveness of security acquisition, implementation, and other program activities • Organize, aggregate, and analyze your data to bring out key insights • Use visualization to understand and communicate security issues more clearly • Capture valuable data from firewalls and antivirus logs, third-party auditor reports, and other resources • Implement balanced scorecards that present compact, holistic views of organizational security effectiveness

Managing Cybersecurity in the Process Industries Academic Conferences Limited

IT Certification Success Exam Cram 2 provides you with a detailed explanation of the certification arena from Ed Tittel, one of the most respected figures in the industry. The book explains the various certification programs, their prerequisites, what can be done with them, and where you might want to go next. Readers preparing for a certification exam find the best-selling Exam Cram 2 series to be the smartest, most efficient way to become certified. This book focuses exactly on what you need to know to get certified now!

The Measurement and Analysis of Housing Preference and Choice Prabhat Prakashan

These proceedings represent the work of contributors to the 16th International Conference on Cyber Warfare and Security (ICCWS 2021), hosted by joint collaboration of Tennessee Tech Cybersecurity Education, Research and Outreach Center (CEROC), Computer Science department and the Oak Ridge National Laboratory, Tennessee on 25-26 February 2021. The Conference Co-Chairs are Dr. Juan Lopez Jr, Oak Ridge National Laboratory, Tennessee, and Dr. Ambareen Siraj, Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC), and the Program Chair is Dr. Kalyan Perumalla, from Oak Ridge National Laboratory, Tennessee.

Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions "O'Reilly Media, Inc."

Many people think of the Smart Grid as a power distribution group built on advanced smart metering—but that's just one aspect of a much larger and more complex system. The "Smart Grid" requires new technologies throughout energy generation, transmission and distribution, and even the homes and businesses being served by the grid. This also represents new information paths between these new systems and services, all of which represents risk, requiring a more thorough approach to where and how cyber security controls are implemented. This insight provides a detailed architecture of the entire Smart Grid, with recommended cyber security measures for everything from the supply chain to the consumer. Discover the potential of the Smart Grid Learn in depth about its systems See its vulnerabilities and how best to protect it

UNIX Systems Programming for SVR4 Lulu.com

Cyberattack-an ominous word that strikes fear in the hearts of nearly everyone, especially business owners, CEOs, and executives. With cyberattacks resulting in often devastating results, it's no wonder executives hire the best and brightest of the IT world for protection. But are you doing enough? Do you understand your risks? What if the brightest aren't always the best choice for your company? In The Smartest Person in the Room, Christian Espinosa shows you how to leverage your company's smartest minds to your benefit and theirs. Learn from Christian's own journey from cybersecurity engineer to company CEO. He describes why a high IQ is a lost superpower when effective communication, true intelligence, and self-confidence

are not embraced. With his seven-step methodology and stories from the field, Christian helps you develop your team's technical minds so they become better humans and strong leaders who excel in every role. This book provides you with an enlightening perspective of how to turn your biggest unknown weakness into your strongest defense.
IT Certification Success Exam Cram 2 Hudson Whitman/ ECP
Applied Cyber Security and the Smart GridNewnes
Cybercrime Investigations Que Publishing
Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security helps individuals take control of their cybersecurity. Every day in the news, we see cybercrime -- a multi-billion-dollar-a-year criminal industry whose actors have little fear of law enforcement.
Security Metrics Addison-Wesley Professional
Did you know your car can be hacked? Your medical device? Your employer’s HVAC system? Are you aware that bringing your own device to work may have security implications? Consumers of digital technology are often familiar with headline-making hacks and breaches, but lack a complete understanding of how and why they happen, or if they have been professionally or personally compromised. In Cybersecurity in Our Digital Lives, twelve experts provide much-needed clarification on the technology behind our daily digital interactions. They explain such things as supply chain, Internet of Things, social media, cloud computing, mobile devices, the C-Suite, social engineering, and legal confidentially. Then, they discuss very real threats, make suggestions about what can be done to enhance security, and offer recommendations for best practices. An ideal resource for students, practitioners, employers, and anyone who uses digital products and services.
Proceedings of the 16th International Conference on Cyber Warfare and Security-ICCWS 2021 Prentice Hall
The chemical process industry is a rich target for cyber attackers who are intent on causing harm. Current risk management techniques are based on the premise that events are initiated by a single failure and the succeeding sequence of events is predictable. A cyberattack on the Safety, Controls, Alarms, and Interlocks (SCAI) undermines this basic assumption. Each facility should have a Cybersecurity Policy, Implementation Plan and Threat Response Plan in place. The response plan should address how to bring the process to a safe state when controls and safety systems are compromised. The emergency response plan should be updated to reflect different actions that may be appropriate in a sabotage situation. IT professionals, even those working at chemical facilities are primarily focused on the risk to business systems. This book contains guidelines for companies on how to improve their process safety performance by applying Risk Based Process Safety (RBPS) concepts and techniques to the problem of cybersecurity.