

Get Free Cyber Security Online Training Courses

Cyber Security Online Training Courses

CompTIA Security+ Study Guide
(Exam SY0-601)

This book is a practical guide to discovering and exploiting security flaws in web applications. The authors explain each category of vulnerability using real-world examples, screen shots and code extracts. The book is extremely practical in focus, and describes in detail the steps involved in detecting and exploiting each kind of security weakness found within a variety of applications such as online banking, e-commerce and other web applications. The topics covered

Get Free Cyber Security Online Training Courses

include bypassing login mechanisms, injecting code, exploiting logic flaws and compromising other users. Because every web application is different, attacking them entails bringing to bear various general principles, techniques and experience in an imaginative way. The most successful hackers go beyond this, and find ways to automate their bespoke attacks. This handbook describes a proven methodology that combines the virtues of human intelligence and computerized brute force, often with devastating results. The authors are professional penetration testers who have been involved in web application security

Get Free Cyber Security Online Training Courses

for nearly a decade. They have presented training courses at the Black Hat security conferences throughout the world. Under the alias "PortSwigger", Dafydd developed the popular Burp Suite of web application hack tools.

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. This effective study guide provides 100% coverage of every topic on the latest version of the CISM exam Written by an information security executive consultant, experienced author, and university instructor, this highly

Get Free Cyber Security Online Training Courses

effective integrated self-study system enables you to take the challenging CISM exam with complete confidence. CISM Certified Information Security Manager All-in-One Exam Guide covers all four exam domains developed by ISACA. You'll find learning objectives at the beginning of each chapter, exam tips, practice questions, and in-depth explanations. All questions closely match those on the live test in tone, format, and content. "Note," "Tip," and "Caution" sections throughout provide real-world insight and call out potentially harmful situations. Beyond fully preparing you for the exam, the book also serves as a

Get Free Cyber Security Online Training Courses

valuable on-the-job reference.

Covers all exam domains, including:

- Information security governance •
 - Information risk management •
 - Information security program development and management •
 - Information security incident management
- Electronic content includes:
- 400 practice exam questions •
 - Test engine that provides full-length practice exams and customizable quizzes by exam topic •
 - Secured book PDF

Your career as a Penetration Tester begins here with the REVISED

CompTIA PenTest+ Study Guide!

CompTIA PenTest+ Study Guide:

Exam PT0-002, Second Edition,

introduces you to the core skills and

Get Free Cyber Security Online Training Courses

techniques that every pen tester needs: Perform assessments of traditional server and desktop operating systems as well as new types of network devices, including mobile, cloud, IoT, industrial, and embedded Identify security weaknesses Manage system vulnerabilities Determine if existing cybersecurity practices deviate from accepted practices, configurations and policies Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. Typical penetration testing

Get Free Cyber Security Online Training Courses

consists of low-level hackers attacking a system with a list of known vulnerabilities, and defenders preventing those hacks using an equally well-known list of defensive scans. Readers will also have access to additional online study tools, including hundreds of bonus practice exam questions, electronic flashcards, and a searchable Glossary of important terms. Prepare smarter with Sybex's superior interactive online learning environment and test bank.

Best Practices for Designing, Implementing, and Maintaining Systems

Discovering and Exploiting Security Flaws

Get Free Cyber Security Online Training Courses

CompTIA Security+ (exam SYO-301)

Learn Ethical Hacking from Scratch

CompTIA PenTest+ Study Guide

Cyber Security Essentials

Totally updated for 2011, here's the ultimate study guide for the CISSP exam. Considered the most desired certification for IT security professionals, the Certified Information Systems Security Professional designation is also a career-booster. This comprehensive study guide covers every aspect of the 2011 exam and the latest revision of the CISSP body of knowledge.

Get Free Cyber Security Online Training Courses

It offers advice on how to pass each section of the exam and features expanded coverage of biometrics, auditing and accountability, software security testing, and other key topics. Included is a CD with two full-length, 250-question sample exams to test your progress. CISSP certification identifies the ultimate IT security professional; this complete study guide is fully updated to cover all the objectives of the 2011 CISSP exam Provides in-depth knowledge of access

Get Free Cyber Security Online Training Courses

control, application development security, business continuity and disaster recovery planning, cryptography, Information Security governance and risk management, operations security, physical (environmental) security, security architecture and design, and telecommunications and network security Also covers legal and regulatory investigation and compliance Includes two practice exams and challenging review questions on the CD

Get Free Cyber Security Online Training Courses

Professionals seeking the CISSP certification will boost their chances of success with CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition.

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

Get Free Cyber Security Online Training Courses

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

Get Free Cyber Security Online Training Courses

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

Get Free Cyber Security Online Training Courses

*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*

As a result of a rigorous, methodical process that (ISC) follows to routinely update its credential exams, it has announced that enhancements will be made to both the Certified Information Systems Security Professional (CISSP) credential,

Get Free Cyber Security Online Training Courses

*beginning April 15, 2015.
(ISC) conducts this process on a regular basis to ensure that the examinations and
The sophisticated methods used in recent high-profile cyber incidents have driven many to need to understand how such security issues work.
Demystifying the complexity often associated with information assurance,
Cyber Security Essentials provides a clear understanding of the concepts behind prevalent threats, tactics, and*

Get Free Cyber Security Online Training Courses

*procedures. To accomplish
Defensive Security
Handbook*

*Exam Core 1 220-1001 and
Exam Core 2 220-1002*

*Cellular Convergence and
the Death of Privacy
CISSP: Certified*

*Information Systems
Security Professional
Study Guide*

*Hacker Techniques, Tools,
and Incident Handling*

*Building a Modern Computer
from First Principles*

***Cyber Security Engineering is
the definitive modern reference
and tutorial on the full range of
capabilities associated with
modern cyber security***

engineering. Pioneering software

Get Free Cyber Security Online Training Courses

assurance experts Dr. Nancy R. Mead and Dr. Carol C. Woody bring together comprehensive best practices for building software systems that exhibit superior operational security, and for considering security throughout your full system development and acquisition lifecycles. Drawing on their pioneering work at the Software Engineering Institute (SEI) and Carnegie Mellon University, Mead and Woody introduce seven core principles of software assurance, and show how to apply them coherently and systematically. Using these principles, they help you prioritize the wide range of possible security actions available to you, and justify the

Get Free Cyber Security Online Training Courses

required investments. Cyber Security Engineering guides you through risk analysis, planning to manage secure software development, building organizational models, identifying required and missing competencies, and defining and structuring metrics. Mead and Woody address important topics, including the use of standards, engineering security requirements for acquiring COTS software, applying DevOps, analyzing malware to anticipate future vulnerabilities, and planning ongoing improvements. This book will be valuable to wide audiences of practitioners and managers with responsibility for systems, software, or quality engineering, reliability, security,

Get Free Cyber Security Online Training Courses

acquisition, or operations.

Whatever your role, it can help you reduce operational problems, eliminate excessive patching, and deliver software that is more resilient and secure.

Ace preparation for the CompTIA Security+ Exam SY0-301 with this 2-in-1 Training Kit from Microsoft Press]. Features a series of lessons and practical exercises to maximize performance with customizable testing options.

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.

Get Free Cyber Security Online Training Courses

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

Get Free Cyber Security Online Training Courses

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-

Get Free Cyber Security Online Training Courses

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. Originally published in hardcover in 2016 by Simon & Schuster. A Beginner's Guide

Get Free Cyber Security Online Training Courses

Your stepping stone to penetration testing

Your Blueprint to Financial Independence

Android Forensics

The Secret History of Cyber War

A Practical Approach for Systems and Software Assurance

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

Get Free Cyber Security Online Training Courses

personal.

Now available for Pre-Order! A common resolution set at the beginning of a new year is to "get my financial house in order." But how can you build a house, let alone pour any kind of foundation, without a blueprint? There are dozens of books and gurus trying to push their advice and tell you how to spend and invest your money. And then, there are three suburban dads just trying to make the world a little bit better. Meet Brad Barrett and Jonathan Mendonsa of the award-winning ChooseFI podcast and Chris Mamula of the popular blog "Can I Retire Yet?". They have walked the talk and now want to share their knowledge with you. Together, these three regular guys will show you how they did something extraordinary. They are all financially independent and doing meaningful work that fulfills them. All three left their corporate 9 to 5 jobs and are reaping the

Get Free Cyber Security Online Training Courses

benefits of extra time with their families. Mirroring the format of the popular ChooseFI podcast, this book pulls from the collective knowledge of those who have decided to build a lifestyle around their passions instead of allowing their finances to dictate their future. These stories demonstrate universal principles, giving you the opportunity to pick the elements that are the most applicable to your financial situation and "choose your own adventure." The book covers a wide range of topics that will help you build a strong financial foundation: Developing a growth mindset Defining your values and aligning them with your spending Cutting years from your estimated retirement date Questioning the status quo on "required expenses" Cutting travel expenses and putting family vacations within your reach Learning how to earn more and live with abundance Updating the commonly accepted wisdom on college

Get Free Cyber Security Online Training Courses

education and the debt associated with it Cutting through the noise on investing to discover strategies that work Showing how to implement investment strategies that enable the lifestyle you desire while controlling downside risk FI or Financial Independence is the new debt-free and getting back to 0 is just the beginning of a wonderful journey. Whether you have mountains of debt now or are recently debt free and wondering what to do next, Choose FI: Your Blueprint to Financial Independence will give you the information to guide your next move.

Provides a basic overview of the employment status of women in the cybersecurity field.

The open source nature of the platform has not only established a new direction for the industry, but enables a developer or forensic analyst to understand the device at the most fundamental level. Android Forensics

Get Free Cyber Security Online Training Courses

covers an open source mobile device platform based on the Linux 2.6 kernel and managed by the Open Handset Alliance. The Android platform is a major source of digital forensic investigation and analysis. This book provides a thorough review of the Android platform including supported hardware devices, the structure of the Android development project and implementation of core services (wireless communication, data storage and other low-level functions). Finally, it will focus on teaching readers how to apply actual forensic techniques to recover data. Ability to forensically acquire Android devices using the techniques outlined in the book Detailed information about Android applications needed for forensics investigations Important information about SQLite, a file based structured data storage relevant for both Android and many other platforms.

Get Free Cyber Security Online Training Courses

CISM Certified Information Security

Manager All-in-One Exam Guide

CompTIA A+ Complete Practice Tests

Official (ISC)2® Guide to the

CISSP®-ISSEP® CBK®

Best Practices for Securing Infrastructure

CASP+ CompTIA Advanced Security

Practitioner Study Guide

What Every Programmer Needs to Know

As digital crime increases exponentially, the need for investigative expertise in both government and civilian sectors has increased proportionally as well. The Network Defense and Investigations course textbook provides students with methods and strategies to mitigate incident damage with efficient and effective response procedures, acquire

Get Free Cyber Security Online Training Courses

digital evidence in a forensically sound manner, identify and analyze the recovered evidence for relevant facts, and document and report details of the investigation in a manner consistent with professional industry standards. In many cases, the cybersecurity professional must also be prepared to offer expert witness testimony in civil and legal venues. Comprised of 14 detailed chapters designed to align to academic calendars, students are presented with topics such as Enterprise Network Devices and Services, Host and Network Investigations, Memory Forensics, Evidence

Get Free Cyber Security Online Training Courses

Collection, Forensic Analysis, Chain of Custody standards, and Reporting and Documentation requirements. Immersive learning labs utilize the Project Ares® Cyber Range and Wireshark network protocol analyzer software.

Cybercrime continues to skyrocket but we are not combatting it effectively yet. We need more cybercrime investigators from all backgrounds and working in every sector to conduct effective investigations. This book is a comprehensive resource for everyone who encounters and investigates cybercrime, no matter their title, including those working

Get Free Cyber Security Online Training Courses

on behalf of law enforcement, private organizations, regulatory agencies, or individual victims. It provides helpful background material about cybercrime's technological and legal underpinnings, plus in-depth detail about the legal and practical aspects of conducting cybercrime investigations. Key features of this book include: Understanding cybercrime, computers, forensics, and cybersecurity Law for the cybercrime investigator, including cybercrime offenses; cyber evidence-gathering; criminal, private and regulatory law, and nation-state implications Cybercrime

Get Free Cyber Security Online Training Courses

investigation from three key perspectives: law enforcement, private sector, and regulatory Financial investigation Identification (attribution) of cyber-conduct Apprehension Litigation in the criminal and civil arenas. This far-reaching book is an essential reference for prosecutors and law enforcement officers, agents and analysts; as well as for private sector lawyers, consultants, information security professionals, digital forensic examiners, and more. It also functions as an excellent course book for educators and trainers. We need more investigators who know how to fight cybercrime,

Get Free Cyber Security Online Training Courses

and this book was written to achieve that goal. Authored by two former cybercrime prosecutors with a diverse array of expertise in criminal justice and the private sector, this book is informative, practical, and readable, with innovative methods and fascinating anecdotes throughout.

The only official, comprehensive reference guide to the CISSP

Thoroughly updated for 2021 and beyond, this is the authoritative common body of knowledge (CBK) from (ISC)2 for information security professionals charged with designing, engineering, implementing, and managing

Get Free Cyber Security Online Training Courses

the overall information security program to protect organizations from increasingly sophisticated attacks. Vendor neutral and backed by (ISC)2, the CISSP credential meets the stringent requirements of ISO/IEC Standard 17024. This CBK covers the current eight domains of CISSP with the necessary depth to apply them to the daily practice of information security. Revised and updated by a team of subject matter experts, this comprehensive reference covers all of the more than 300 CISSP objectives and sub-objectives in a structured format with: Common and good practices for each

Get Free Cyber Security Online Training Courses

objective Common vocabulary and definitions References to widely accepted computing standards Highlights of successful approaches through case studies Whether you've earned your CISSP credential or are looking for a valuable resource to help advance your security career, this comprehensive guide offers everything you need to apply the knowledge of the most recognized body of influence in information security Provides information on ways to use Wireshark to capture and analyze packets, covering such topics as building customized capture and display filters, graphing

Get Free Cyber Security Online Training Courses

traffic patterns, and building statistics and reports.

Cybersecurity Blue Team Toolkit

Official (ISC)2 Guide to the CISSP CBK

Using Python for Cyber Offense and Defense

Chained Exploits

Investigation, Analysis, and Mobile Security for Google Android

Hands on Hacking

An accessible introduction to cybersecurity concepts and practices Cybersecurity Essentials provides a comprehensive introduction to the field, with expert coverage of essential topics required for

Get Free Cyber Security Online Training Courses

entry-level cybersecurity certifications. An effective defense consists of four distinct challenges: securing the infrastructure, securing devices, securing local networks, and securing the perimeter. Overcoming these challenges requires a detailed understanding of the concepts and practices within each realm. This book covers each challenge individually for greater depth of information, with real-world scenarios that show what vulnerabilities look like in everyday computing scenarios. Each part concludes with a summary of key concepts,

Get Free Cyber Security Online Training Courses

review questions, and hands-on exercises, allowing you to test your understanding while exercising your new critical skills. Cybersecurity jobs range from basic configuration to advanced systems analysis and defense assessment. This book provides the foundational information you need to understand the basics of the field, identify your place within it, and start down the security certification path. Learn security and surveillance fundamentals Secure and protect remote access and devices Understand network topologies, protocols, and strategies Identify threats

Get Free Cyber Security Online Training Courses

and mount an effective defense Cybersecurity Essentials gives you the building blocks for an entry level security certification and provides a foundation of cybersecurity knowledge Cybersecurity is undoubtedly one of the fastest-growing fields. However, there is an acute shortage of skilled workforce. The cybersecurity beginners guide aims at teaching security enthusiasts all about organizational digital assets' security, give them an overview of how the field operates, applications of cybersecurity across sectors and industries, and skills and

Get Free Cyber Security Online Training Courses

certifications one needs to build and scale up a career in this field.

Cellular technology has always been a surveillance technology, but "cellular convergence" - the growing trend for all forms of communication to consolidate onto the cellular handset - has dramatically increased the impact of that surveillance. In *Cellular Convergence and the Death of Privacy*, Stephen Wicker explores this unprecedented threat to privacy from three distinct but overlapping perspectives: the technical, the legal, and the social. Professor Wicker first

Get Free Cyber Security Online Training Courses

describes cellular technology and cellular surveillance using language accessible to non-specialists. He then examines current legislation and Supreme Court jurisprudence that form the framework for discussions about rights in the context of cellular surveillance. Lastly, he addresses the social impact of surveillance on individual users. The story he tells is one of a technology that is changing the face of politics and economics, but in ways that remain highly uncertain.

A practical guide to deploying digital forensic techniques in response to cyber security

Get Free Cyber Security Online Training Courses

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

Get Free Cyber Security Online Training Courses

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

Get Free Cyber Security Online Training Courses

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

Get Free Cyber Security Online Training Courses

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

Get Free Cyber Security Online Training Courses

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.

The Official (ISC)2 CISSP CBK Reference

A Comprehensive Resource for Everyone

Cybersecurity Fundamentals Study Guide

A Dog's Guide to Internet Security

Get Free Cyber Security Online Training Courses

Dark Territory

Women in Cybersecurity

Prepare to succeed in your new cybersecurity career with the challenging and sought-after CASP+ credential In the newly updated Fourth Edition of CASP+ CompTIA Advanced Security Practitioner Study Guide Exam CAS-004, risk management and compliance expert Jeff Parker walks you through critical security topics and hands-on labs designed to prepare you for the new CompTIA Advanced Security Professional exam and a career in cybersecurity implementation. Content and chapter structure of this Fourth edition was developed and restructured to represent the CAS-004 Exam Objectives. From

Get Free Cyber Security Online Training Courses

operations and architecture concepts, techniques and requirements to risk analysis, mobile and small-form factor device security, secure cloud integration, and cryptography, you'll learn the cybersecurity technical skills you'll need to succeed on the new CAS-004 exam, impress interviewers during your job search, and excel in your new career in cybersecurity implementation. This comprehensive book offers:

Efficient preparation for a challenging and rewarding career in implementing specific solutions within cybersecurity policies and frameworks A robust grounding in the technical skills you'll need to impress during cybersecurity interviews Content delivered through scenarios, a strong focus

Get Free Cyber Security Online Training Courses

of the CAS-004 Exam Access to an interactive online test bank and study tools, including bonus practice exam questions, electronic flashcards, and a searchable glossary of key terms Perfect for anyone preparing for the CASP+ (CAS-004) exam and a new career in cybersecurity, CASP+ CompTIA Advanced Security Practitioner Study Guide Exam CAS-004 is also an ideal resource for current IT professionals wanting to promote their cybersecurity skills or prepare for a career transition into enterprise cybersecurity. Everybody says be careful online, but what do they mean? Lacey is a cyber-smart dog who protects kids by teaching them how to stay safe online. Join Lacey and her friend Gabbi on a fun, cyber safe

Get Free Cyber Security Online Training Courses

adventure and learn the ins and outs of how to behave and how to keep yourself safe online. In this day in age our kids are accessing the internet about as soon as they can read! Cyber Safe is a fun way to ensure they understand their surroundings in our digital world. Prepare for the CompTIA CySA+ certification exam with this fully updated self-study resource This highly effective self-study system provides complete coverage of every objective for the challenging CompTIA CySA+ Cybersecurity Analyst exam. You'll find learning objectives at the beginning of each chapter, exam tips, in-depth explanations, and practice exam questions. All questions closely mirror those on the actual test in content, format, and tone. Designed

Get Free Cyber Security Online Training Courses

to help you pass the CS0-002 exam with ease, this definitive guide also serves as an essential on-the-job reference. Covers all exam topics, including: Threat and vulnerability management Threat data and intelligence Vulnerability management, assessment tools, and mitigation Software and systems security Solutions for infrastructure management Software and hardware assurance best practices Security operations and monitoring Proactive threat hunting Automation concepts and technologies Incident response process, procedure, and analysis Compliance and assessment Data privacy and protection Support of organizational risk mitigation Online content includes: 200+ practice questions Interactive

Get Free Cyber Security Online Training Courses

performance-based questions Test engine that provides full-length practice exams and customizable quizzes by exam objective

The complete guide to today's hard-to-defend chained attacks:

performing them and preventing them Nowadays, it's rare for malicious hackers to rely on just one exploit or tool; instead, they use "chained" exploits that integrate multiple forms of attack to achieve their goals. Chained exploits are far more complex and far more difficult to defend. Few security or hacking books cover them well and most don't cover them at all. Now there's a book that brings together start-to-finish information about today's most widespread chained exploits—both how to perform them and how to

Get Free Cyber Security Online Training Courses

prevent them. Chained Exploits demonstrates this advanced hacking attack technique through detailed examples that reflect real-world attack strategies, use today's most common attack tools, and focus on actual high-value targets, including credit card and healthcare data. Relentlessly thorough and realistic, this book covers the full spectrum of attack avenues, from wireless networks to physical access and social engineering. Writing for security, network, and other IT professionals, the authors take you through each attack, one step at a time, and then introduce today's most effective countermeasures– both technical and human. Coverage includes: Constructing convincing new phishing attacks Discovering which

Get Free Cyber Security Online Training Courses

*sites other Web users are visiting
Wreaking havoc on IT security via
wireless networks Disrupting
competitors' Web sites
Performing—and
preventing—corporate espionage
Destroying secure files Gaining
access to private healthcare
records Attacking the viewers of
social networking pages Creating
entirely new exploits and more
Andrew Whitaker, Director of
Enterprise InfoSec and Networking
for Training Camp, has been
featured in The Wall Street Journal
and BusinessWeek. He coauthored
Penetration Testing and Network
Defense. Andrew was a winner of
EC Council's Instructor of
Excellence Award. Keatron Evans is
President and Chief Security
Consultant of Blink Digital Security,*

Get Free Cyber Security Online Training Courses

LLC, a trainer for Training Camp, and winner of EC Council's Instructor of Excellence Award. Jack B. Voth specializes in penetration testing, vulnerability assessment, and perimeter security. He co-owns The Client Server, Inc., and teaches for Training Camp throughout the United States and abroad.
informit.com/aw Cover photograph

© Corbis / Jupiter Images

Using Wireshark to Solve Real-world Network Problems

Exam PT0-002

Schneier on Security

Network Defense and Investigations

Foundations of Security

The Web Application Hacker's Handbook

Can a system be considered truly reliable if it isn't

Get Free Cyber Security Online Training Courses

fundamentally secure? Or can it be considered secure if it's unreliable? Security is crucial to the design and operation of scalable systems in production, as it plays an important part in product quality, performance, and availability. In this book, experts from Google share best practices to help your organization design scalable and reliable systems that are fundamentally secure. Two previous O'Reilly books from Google—Site Reliability Engineering and The Site Reliability Workbook—demonstrated how and why a commitment to the entire service lifecycle

Get Free Cyber Security Online Training Courses

enables organizations to successfully build, deploy, monitor, and maintain software systems. In this latest guide, the authors offer insights into system design, implementation, and maintenance from practitioners who specialize in security and reliability. They also discuss how building and adopting their recommended best practices requires a culture that's supportive of such change. You'll learn about secure and reliable systems through: Design strategies Recommendations for coding, testing, and debugging practices Strategies to prepare for, respond to, and

Get Free Cyber Security Online Training Courses

recover from incidents
Cultural best practices that help teams across your organization collaborate effectively

Test your knowledge and know what to expect on A+ exam day CompTIA A+ Complete Practice Tests, Second Edition enables you to hone your test-taking skills, focus on challenging areas, and be thoroughly prepared to ace the exam and earn your A+ certification. This essential component of your overall study plan presents nine unique practice tests—and two 90-question bonus tests—covering 100% of the objective domains for both the 220-1001 and

Get Free Cyber Security Online Training Courses

220-1002 exams.

Comprehensive coverage of every essential exam topic ensures that you will know what to expect on exam day and maximize your chances for success. Over 1200 practice questions on topics including hardware, networking, mobile devices, operating systems and procedures, troubleshooting, and more, lets you assess your performance and gain the confidence you need to pass the exam with flying colors. This second edition has been fully updated to reflect the latest best practices and updated exam objectives you will see on the big day. A+

Get Free Cyber Security Online Training Courses

certification is a crucial step in your IT career. Many businesses require this accreditation when hiring computer technicians or validating the skills of current employees. This collection of practice tests allows you to:

- Access the test bank in the Sybex interactive learning environment
- Understand the subject matter through clear and accurate answers and explanations of exam objectives
- Evaluate your exam knowledge and concentrate on problem areas
- Integrate practice tests with other Sybex review and study guides, including the CompTIA A+ Complete Study

Get Free Cyber Security Online Training Courses

Guide and the CompTIA A+ Complete Deluxe Study Guide Practice tests are an effective way to increase comprehension, strengthen retention, and measure overall knowledge. The CompTIA A+ Complete Practice Tests, Second Edition is an indispensable part of any study plan for A+ certification.

Modern society has become dependent on technology, allowing personal information to be input and used across a variety of personal and professional systems. From banking to medical records to e-commerce, sensitive data has never before been at such a

Get Free Cyber Security Online Training Courses

high risk of misuse. As such, organizations now have a greater responsibility than ever to ensure that their stakeholder data is secured, leading to the increased need for cybersecurity specialists and the development of more secure software and systems. To avoid issues such as hacking and create a safer online space, cybersecurity education is vital and not only for those seeking to make a career out of cybersecurity, but also for the general public who must become more aware of the information they are sharing and how they are using it. It is crucial people learn

Get Free Cyber Security Online Training Courses

about cybersecurity in a comprehensive and accessible way in order to use the skills to better protect all data. The Research Anthology on Advancements in Cybersecurity Education discusses innovative concepts, theories, and developments for not only teaching cybersecurity, but also for driving awareness of efforts that can be achieved to further secure sensitive data. Providing information on a range of topics from cybersecurity education requirements, cyberspace security talents training systems, and insider threats, it is ideal for educators, IT

Get Free Cyber Security Online Training Courses

developers, education professionals, education administrators, researchers, security analysts, systems engineers, software security engineers, security professionals, policymakers, and students.

Learn how to hack systems like black hat hackers and secure them like security experts

Key Features

Understand how computer systems work and their vulnerabilities

Exploit weaknesses and hack into machines to test their security

Learn how to secure systems from hackers

Book Description

This book starts with the basics of ethical hacking, how to practice

Get Free Cyber Security Online Training Courses

hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking, where you will see how to test the security of wired and wireless networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks. You will also get the hang of post-exploitation techniques, including remotely controlling and interacting

Get Free Cyber Security Online Training Courses

with the systems that you compromised. Towards the end of the book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the different fields and types

Get Free Cyber Security Online Training Courses

of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how

Get Free Cyber Security Online Training Courses

to hack and test the security of systems like professional hackers and security experts.

LabSim for Security Pro
Choose FI

Research Anthology on
Advancements in
Cybersecurity Education
Digital Forensics and

Incident Response

The Official CompTIA

Security+ Self-Paced Study
Guide (Exam SY0-601)

Advanced Hacking Attacks
from Start to Finish

Software developers need to worry about security as never before. They need clear guidance on safe coding practices, and that ' s exactly what this book delivers.

The book does not delve deep into

Get Free Cyber Security Online Training Courses

theory, or rant about the politics of security. Instead, it clearly and simply lays out the most common threats that programmers need to defend against. It then shows programmers how to make their defense. The book takes a broad focus, ranging over SQL injection, worms and buffer overflows, password security, and more. It sets programmers on the path towards successfully defending against the entire gamut of security threats that they might face. This title gives students an integrated and rigorous picture of applied computer science, as it comes to play in the construction of a simple yet powerful computer system.

The Official (ISC)² Guide to the CISSP-ISSEP CBK provides an inclusive analysis of all of the topics covered on

Get Free Cyber Security Online Training Courses

the newly created CISSP-ISSEP Common Body of Knowledge. The first fully comprehensive guide to the CISSP-ISSEP CBK, this book promotes understanding of the four ISSEP domains: Information Systems Security Engineering (ISSE); Certifica

A practical handbook to cybersecurity for both tech and non-tech professionals As reports of major data breaches fill the headlines, it has become impossible for any business, large or small, to ignore the importance of cybersecurity. Most books on the subject, however, are either too specialized for the non-technical professional or too general for positions in the IT trenches. Thanks to author Nadean Tanner ' s wide array of experience from teaching at a University to working for the Department of

Get Free Cyber Security Online Training Courses

Defense, the Cybersecurity Blue Team Toolkit strikes the perfect balance of substantive and accessible, making it equally useful to those in IT or management positions across a variety of industries. This handy guide takes a simple and strategic look at best practices and tools available to both cybersecurity management and hands-on professionals, whether they be new to the field or looking to expand their expertise. Tanner gives comprehensive coverage to such crucial topics as security assessment and configuration, strategies for protection and defense, offensive measures, and remediation while aligning the concept with the right tool using the CIS Controls version 7 as a guide. Readers will learn why and how to use fundamental open source and free

Get Free Cyber Security Online Training Courses

tools such as ping, tracert, PuTTY, pathping, sysinternals, NMAP, OpenVAS, Nexpose Community, OSSEC, Hamachi, InSSIDer, Nexpose Community, Wireshark, Solarwinds Kiwi Syslog Server, Metasploit, Burp, Clonezilla and many more. Up-to-date and practical cybersecurity instruction, applicable to both management and technical positions

- Straightforward explanations of the theory behind cybersecurity best practices
- Designed to be an easily navigated tool for daily use
- Includes training appendix on Linux, how to build a virtual lab and glossary of key terms

The Cybersecurity Blue Team Toolkit is an excellent resource for anyone working in digital policy as well as IT security professionals, technical analysts, program managers,

Get Free Cyber Security Online Training Courses

and Chief Information and Technology Officers. This is one handbook that won't gather dust on the shelf, but remain a valuable reference at any career level, from student to executive.

Cyber Safe

CompTIA CySA+ Cybersecurity

Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002)

Practical Packet Analysis

Training Kit

Cyber Security Engineering

The Elements of Computing Systems

This book provides a structured, hands-on introduction to using Python for cybersecurity. With the MITRE ATT&CK framework as a guide, readers will explore the lifecycle of a cyberattack and see how Python code can be

Get Free Cyber Security Online Training Courses

used to solve key challenges at each stage of the process. Each application will be explored from the perspective of both the attacker and the defender, showing how Python can be used to automate attacks and to detect and prevent them. By following the MITRE ATT&CK framework, this book explores the use of Python for a number of cybersecurity uses cases, including: Intelligence collection Exploitation and lateral movement Persistence and privilege escalation Command and control Extraction and encryption of valuable data Each use case will include ready-to-

Get Free Cyber Security Online Training Courses

run code samples and demonstrations of their use in a target environment. Readers will gain hands-on experience in applying Python to cybersecurity use cases and practice in creating and adapting Python code to address novel situations. Hacker Techniques, Tools, and Incident Handling, Third Edition begins with an examination of the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals who break into networks, steal information, and corrupt data. It goes on to review the technical overview of

Get Free Cyber Security Online Training Courses

hacking: how attacks target networks and the methodology they follow. The final section studies those methods that are most effective when dealing with hacking attacks, especially in an age of increased reliance on the Web. Written by subject matter experts, with numerous real-world examples, *Hacker Techniques, Tools, and Incident Handling, Third Edition* provides readers with a clear, comprehensive introduction to the many threats on our Internet environment and security and what can be done to combat them.

Exam CAS-004

Page 76/77

Get Free Cyber Security Online Training Courses

Cybersecurity Essentials
Building Secure and Reliable
Systems

An Introduction to Cyber Security
Python for Cybersecurity
Cybercrime Investigations