Offensive Security

How do you use Offensive Security Exploitation Expert data and information to support organizational decision making and innovation? How important is Offensive Security Exploitation Expert to the user organizations mission? Which customers cant participate in our Offensive Security Exploitation Expert domain because they lack skills, wealth, or convenient access to existing solutions? Does our organization need more Offensive Security Exploitation Expert education? Are we making progress? and are we making progress as Offensive Security Exploitation Expert leaders? This amazing Offensive Security Exploitation Expert self-assessment will make you the accepted Offensive Security Exploitation Expert domain auditor by revealing just what you need to know to be fluent and ready for any Offensive Security Exploitation Expert challenge. How do I reduce the effort in the Offensive Security Exploitation Expert work to be done to get problems solved? How can I ensure that plans of action include every Offensive Security Exploitation Expert task and that every Offensive Security Exploitation Expert outcome is in place? How will I save time investigating strategic and tactical options and ensuring Offensive Security Exploitation Expert costs are low? How can I deliver tailored Offensive Security Exploitation Expert advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Offensive Security

Exploitation Expert essentials are covered, from every angle: the Offensive Security Exploitation Expert self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Offensive Security Exploitation Expert outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Offensive Security Exploitation Expert practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Offensive Security Exploitation Expert are maximized with professional results. Your purchase includes access details to the Offensive Security Exploitation Expert self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard, and... - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation ...plus an extra, special, resource that helps you with project managing. INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

Harden your business against internal and external cybersecurity threats with a single accessible resource. In 8 Steps to Better Security: A Simple Cyber Resilience Guide for Business, cybersecurity researcher and writer Kim Crawley delivers a grounded and practical roadmap to cyber resilience in any organization. Offering you the lessons she learned while working for major tech companies like Sophos, AT&T, BlackBerry Cylance, Tripwire, and Venafi, Crawley condenses the essence of business cybersecurity into eight steps. Written to be accessible to non-technical businesspeople as well as security professionals, and with insights from other security industry leaders, this important book will walk you through how to: Foster a strong security culture that extends from the custodial team to the C-suite Build an effective security team, regardless of the size or nature of your business Comply with regulatory requirements, including general data privacy rules and industry-specific legislation Test your cybersecurity, including third-party penetration testing and internal red team specialists Perfect for CISOs, security leaders, non-technical businesspeople, and managers at any level, 8 Steps to Better Security is also a must-have resource for companies of all sizes, and in all industries.

For attackers, aggressive collection of data often leads to the disclosure of infrastructure, initial access techniques, and malware being unceremoniously pulled apart by analysts. The application of machine learning in the defensive space has not only increased the cost of being an attacker, but has also limited a techniques' operational life significantly. In the world that attackers currently find themselves in:1. Mass data collection and analysis is accessible to defensive software, and by extension, defensive analysts2. Machine learning is being used everywhere to accelerate defensive maturityAttackers are always at a disadvantage, as we as humans try to defeat auto-learning systems that use every bypass attempt to learn more about us, and predict future bypass attempts. This is especially true for public research, and static bypasses. However, as we will present here, machine learning isn't just for blue teams. In this book we will show how we can actually use machine learning, neural network algorithms that can allow us as pentesters, red teamers, offensive security analysts, etc. to create programs that can help automate steps in offensive attacks. We will see how simple classification, clustering techniques to RNNs, CNNs, etc. can be used to create offensive security programs that can identify vulnerabilities in systems. This book presents real world examples that can help pentesters and red teamers to learn about these algorithms as well as examples that can allow to understand how to use them.

What could be done to prevent similar incidents from occurring in the future? How do you protect your data? What are the usual timings of incident information disclosure to external parties? Does the work address establishing secure means of communicating with the client about the engagement? Client data in transit: does the work address issues surrounding the transmission of sensitive client data between targets and penetration testers systems in the course of the engagement? This astounding Offensive Security self-assessment will make you the reliable Offensive Security domain master by revealing just what you need to know to be fluent and ready for any Offensive Security challenge. How do I reduce the effort in the Offensive Security work to be done to get problems solved? How can I ensure that plans of action include every Offensive Security task and that every Offensive Security outcome is in place? How will I save time investigating strategic and tactical options and ensuring Offensive Security costs are low? How can I deliver tailored Offensive Security advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Offensive Security essentials are covered, from every angle: the Offensive Security self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Offensive Security outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Offensive Security practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Offensive Security are maximized with professional results. Your purchase includes access details to the Offensive Security self-assessment dashboard download which gives you your dynamically prioritized

projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Offensive Security Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.
This book is a fully focused, structured book providing guidance on developing practical penetration testing skills by demonstrating cutting-edge hacker tools and techniques. It offers you all of the essential lab preparation and testing procedures that reflect real-world attack scenarios from a business perspective, in today's digital age.

Need to know Enumeration.

Are the conditions right for the enabling of a rootkit? Who is reviewing corresponding firewall rules? Do you have a way to detect and mitigate anomalies? What limits does the law of war impose on cyber-attacks? What would an attacker see if he/she attempted to profile your network externally? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Offensive Security investments work better. This Offensive Security All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Offensive Security Self-Assessment. Featuring 996 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Offensive Security improvements can be made. In using the questions you will be better able to: - diagnose Offensive Security projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in Offensive Security and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the

Offensive Security Scorecard, you will develop a clear picture of which Offensive Security areas need attention. Your purchase includes access details to the Offensive Security self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Offensive Security Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

Useful commands to know.

This book constitutes the proceedings of the 6th Conference on Information Technologies and Communication of Ecuador “TIC-EC”, held in Riobamba City from November 21 to 23, 2018, and organized by Universidad Nacional del Chimborazo (UNACH) and its Engineering School, and the Ecuadorian Corporation for the Development of Research and Academia (CEDIA). Considered as one of the most important ICT conferences in Ecuador, it brought together international scholars and practitioners to discuss the development, issues and projections of the use of information and communication technologies in multiple fields of application. Presenting high-quality, peer-reviewed papers, the book discusses the following topics: • Communication networks • Software engineering • Computer sciences • Architecture • Intelligent territory management • IT management • Web technologies • ICT in education • Engineering, industry, and construction with ICT support • Entrepreneurship and innovation at the Academy: a business perspective The authors would like to express their sincere gratitude to the invited speakers for their inspirational talks, to the authors for submitting their work to this conference, and the reviewers for sharing their experience during the selection process.

Get up to speed with various penetration testing techniques and resolve security threats of varying complexity Key Features Enhance your penetration testing skills to tackle security threats Learn to gather information, find vulnerabilities, and exploit enterprise defenses Navigate secured systems with the most up-to-date version of Kali Linux (2019.1) and Metasploit (5.0.0) Book Description Sending information via the internet is not entirely private, as evidenced by the rise in hacking, malware attacks, and security threats. With the help of this book, you'll learn crucial penetration testing techniques to help you evaluate enterprise defenses. You'll start by understanding each stage of pentesting and deploying target virtual machines, including Linux and Windows. Next, the book will guide you through performing intermediate penetration testing in a controlled environment. With the help of practical use cases, you'll also be able to implement your learning in real-world scenarios. By studying everything from setting up your lab, information gathering and password attacks, through to social engineering and post exploitation, you'll be able to successfully overcome security threats. The book will even help you leverage the best tools, such as Kali Linux, Metasploit, Burp Suite, and other open source pentesting tools to perform these techniques. Toward the later chapters, you'll focus on best practices to quickly resolve security threats. By the end of this book, you'll be well versed with various penetration testing techniques so as to be able to tackle security threats effectively What you will learn Perform entry-level penetration tests by learning various concepts and techniques Understand both common and not-so-common vulnerabilities from an attacker's perspective Get familiar with intermediate attack methods that can be used in real-world scenarios Understand how vulnerabilities are created by developers and how to fix some of them at source code level Become well versed with basic tools for ethical hacking purposes Exploit known vulnerable services with tools such as Metasploit Who this book is for If you’re just getting started with penetration testing and want to explore various security domains, this book is for you. Security professionals, network engineers, and amateur ethical hackers will also find this book useful. Prior knowledge of penetration testing and ethical hacking is not necessary.

Master the art of exploiting advanced web penetration techniques with Kali Linux 2016.2 About This Book Make the most out of advanced web pen-testing techniques using Kali Linux 2016.2 Explore how Stored (a.k.a. Persistent) XSS attacks work and how to take advantage of them Learn to secure your application by performing advanced web based attacks. Bypass internet security to traverse from the web to a private network. Who This Book Is For This book targets IT pen testers, security consultants, and ethical hackers who want to expand their knowledge and gain expertise on advanced web penetration techniques. Prior knowledge of penetration testing would be beneficial. What You Will Learn Establish a fully-featured sandbox for test rehearsal and risk-free investigation of applications Enlist open-source information to get a head-start on enumerating account credentials, mapping potential dependencies, and discovering unintended backdoors and exposed information Map, scan, and spider web applications using nmap/zenmap, nikto, arachni, webscarab, w3af, and NetCat for more accurate characterization Proxy web transactions through tools such as Burp Suite, OWASP's ZAP tool, and Vega to uncover application weaknesses and manipulate responses Deploy SQL injection, cross-site scripting, Java vulnerabilities, and overflow attacks using Burp Suite, websploit, and SQLMap to test application robustness Evaluate and test identity, authentication, and authorization schemes and sniff out weak cryptography before the black hats do In Detail You will start by delving into some common web application architectures in use, both in private and public cloud instances. You will also learn about the most common frameworks for testing, such as OWASP OGT version 4, and how to use them to guide your efforts. In the next section, you will be introduced to web pentesting with core tools and you will also see how to make web applications more secure through rigorous penetration tests using advanced features in open source tools. The book will then show you how to better hone your web pentesting skills in safe environments that can ensure low-risk experimentation with the powerful tools and features in Kali Linux that go beyond a typical script-kiddie approach. After establishing how to test these powerful tools safely, you will understand how to better identify vulnerabilities, position and deploy exploits, compromise authentication and authorization, and test the resilience and exposure applications possess. By the end of this book, you will be well-versed with the web service architecture to identify and evade various protection mechanisms that are used on the Web today. You will leave this book with a greater mastery of essential test techniques needed to verify the secure design, development, and operation of your customers' web applications. Style and approach An advanced-level guide filled with real-world examples that will help you take your web application's security to the next level by using Kali Linux 2016.2.

Develop your red team skills by learning essential foundational tactics, techniques, and procedures, and boost the overall security posture of your organization by leveraging the homefield advantage Key Features Build, manage, and measure an offensive red team program Leverage the homefield advantage to stay ahead of your adversaries Understand core adversarial tactics and techniques, and protect pentesters and pentesting assets Book Description It's now more important than ever for organizations to be ready to detect and respond to security events and breaches. Preventive measures alone are not enough for dealing with adversaries. A well-rounded prevention, detection, and response program is required. This book will guide you through the stages of building a red team program, including strategies and homefield advantage opportunities to boost security. The book starts by guiding you through establishing, managing, and measuring a red team program, including effective ways for sharing results and findings to raise awareness. Gradually, you'll learn about progressive operations such as cryptocurrency mining, focused privacy testing, targeting telemetry, and even blue team tooling. Later, you'll discover knowledge graphs and how to build them, then become well-versed with basic to advanced techniques related to hunting for credentials, and learn to automate Microsoft Office and browsers to your advantage. Finally, you'll get to grips with protecting assets using decoys, auditing, and alerting with examples for major operating systems. By the end of this book, you'll have learned how to build, manage, and measure a red team program effectively and be well-versed with the fundamental operational techniques required to enhance your existing skills. What you will learn Understand the risks associated with security breaches Implement strategies for building an effective penetration testing team Map out the homefield using knowledge graphs Hunt credentials using indexing and other practical techniques Gain blue team tooling insights to enhance your red team skills Communicate results and influence decision makers with appropriate data Who this book is for This is one of the few detailed cybersecurity books for penetration testers, cybersecurity analysts, security leaders and strategists, as well as red team members and chief information security officers (CISOs) looking to secure their organizations from adversaries. The program management part of this book will also be useful for beginners in the cybersecurity domain. To get the most out of this book, some penetration testing experience, and software engineering and debugging skills are necessary.

During what time window will testing need to be performed? How does the Security Gateway perform data escaping and data sanitization? Is your privacy policy posted on your youbsite and made available to your customers prior to them providing personal information? Do you consider a fully functional WAF one that optimizes for both performance and security? Could your SWG be a back door? This premium Offensive Security Web Expert self-assessment will make you the accepted Offensive Security Web Expert domain standout by revealing just what you need to know to be fluent and ready for any Offensive Security Web Expert challenge. How do I reduce the effort in the Offensive Security Web Expert work to be done to get problems solved? How can I ensure that plans of action include every Offensive Security Web Expert task and that every Offensive Security Web Expert outcome is in place? How will I save time investigating strategic and tactical options and ensuring Offensive Security Web Expert costs are low? How can I deliver tailored Offensive Security Web Expert advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Offensive Security Web Expert essentials are covered, from every angle: the Offensive Security Web Expert self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Offensive Security Web Expert outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Offensive Security Web Expert practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Offensive Security Web Expert are maximized with professional results. Your purchase includes access details to the Offensive Security Web Expert self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment

Excel Dashboard to get familiar with results generation - In-depth and specific Offensive Security Web Expert Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

The first stop for your security needs when using Go, covering host, network, and cloud security for ethical hackers and defense against intrusion Key Features First introduction to Security with Golang Adopting a Blue Team/Red Team approach Take advantage of speed and inherent safety of Golang Works as an introduction to security for Golang developers Works as a guide to Golang security packages for recent Golang beginners Book Description Go is becoming more and more popular as a language for security experts. Its wide use in server and cloud environments, its speed and ease of use, and its evident capabilities for data analysis, have made it a prime choice for developers who need to think about security. Security with Go is the first Golang security book, and it is useful for both blue team and red team applications. With this book, you will learn how to write secure software, monitor your systems, secure your data, attack systems, and extract information. Defensive topics include cryptography, forensics, packet capturing, and building secure web applications. Offensive topics include brute force, port scanning, packet injection, web scraping, social engineering, and post exploitation techniques. What you will learn Learn the basic concepts and principles of secure programming Write secure Golang programs and applications Understand classic patterns of attack Write Golang scripts to defend against network-level attacks Learn how to use Golang security packages Apply and explore cryptographic methods and packages Learn the art of defending against brute force attacks Secure web and cloud applications Who this book is for Security with Go is aimed at developers with basics in Go to the level that they can write their own scripts and small programs without difficulty. Readers should be familiar with security concepts, and familiarity with Python security applications and libraries is an advantage, but not a necessity.

Cybersecurity jobs confines from basic configuration to advanced systems analysis and defense assessment. Cybersecurity: The Beginner's Guide provides thefundamental information you need to understand the basics of the field, identify your place within it, and start your Cybersecurity career.

Take on the perspective of an attacker with this insightful new resource for ethical hackers, pentesters, and social engineers In The Art of Attack: Attacker Mindset for Security Professionals, experienced physical pentester and social engineer Maxie Reynolds untangles the threads of a useful, sometimes dangerous, mentality. The book shows ethical hackers, social engineers, and pentesters what an attacker mindset is and how to and how to use it to their advantage. Adopting this mindset will result in the improvement of security, offensively and defensively, by allowing you to see your environment objectively through the eyes of an attacker. The book shows you the laws of the mindset and the techniques attackers use, from persistence to “start with the end” strategies and non-linear thinking, that make them so dangerous. You’ll discover: A variety of attacker strategies, including approaches, processes, reconnaissance, privilege escalation, redundant access, and escape techniques The unique tells and signs of an attack and how to avoid becoming a victim of one What the science of psychology tells us about amygdala hijacking and other tendencies that you need to protect against Perfect for red teams, social engineers, pentesters, and ethical hackers seeking to fortify and harden their systems and the systems of their clients, The Art of Attack is an invaluable resource for anyone in the technology security space seeking a one-stop resource that puts them in the mind of an attacker.

Want Red Team offensive advice from the biggest cybersecurity names in the industry? Join our tribe. The Tribe of Hackers team is back with a new guide packed with insights from dozens of the world’s leading Red Team security specialists. With their deep knowledge of system vulnerabilities and innovative solutions for correcting security flaws, Red Team hackers are in high demand. Tribe of Hackers Red Team: Tribal Knowledge from the Best in Offensive Cybersecurity takes the valuable lessons and popular interview format from the original Tribe of Hackers and dives deeper into the world of Red Team security with expert perspectives on issues like penetration testing and ethical hacking. This unique guide includes inspiring interviews from influential security specialists, including David Kennedy, Rob Fuller, Jayson E. Street, and Georgia Weidman, who share their real-world learnings on everything from Red Team tools and tactics to careers and communication, presentation strategies, legal concerns, and more Learn what it takes to secure a Red Team job and to stand out from other candidates Discover how to hone your hacking skills while staying on the right side of the law Get tips for collaborating on documentation and reporting Explore ways to garner support from leadership on your security proposals Identify the most important control to prevent compromising your network Uncover the latest tools for Red Team offensive security Whether you’re new to Red Team security, an experienced practitioner, or ready to lead your own team, Tribe of Hackers Red Team has the real-world advice and practical guidance you need to advance your information security career and ready yourself for the Red Team offensive.

Do you receive and act on actionable intelligence? Do you confirm that your data or intellectual property has not been extracted from your applications? Do you share your custom applications with other users? How confident are you that threat intelligence data sent to the cloud for analysis is secure? Where does the cyber threat analysis discipline fit into the modern Security Operation Center (SOC)? This powerful Offensive Security Certified Professional self-assessment will make you the reliable Offensive

Security Certified Professional domain authority by revealing just what you need to know to be fluent and ready for any Offensive Security Certified Professional challenge. How do I reduce the effort in the Offensive Security Certified Professional work to be done to get problems solved? How can I ensure that plans of action include every Offensive Security Certified Professional task and that every Offensive Security Certified Professional outcome is in place? How will I save time investigating strategic and tactical options and ensuring Offensive Security Certified Professional costs are low? How can I deliver tailored Offensive Security Certified Professional advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Offensive Security Certified Professional essentials are covered, from every angle: the Offensive Security Certified Professional self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Offensive Security Certified Professional outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Offensive Security Certified Professional practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Offensive Security Certified Professional are maximized with professional results. Your purchase includes access details to the Offensive Security Certified Professional self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Offensive Security Certified Professional Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips. Build your own secure enterprise or home penetration testing lab to dig into the various hacking techniques About This Book Design and build an extendable penetration testing lab with wireless access suitable for home and enterprise use Fill the lab with various components and customize them according to your own needs and skill level Secure your lab from unauthorized access and external attacks Who This Book Is For If you are a beginner or a security professional who wishes to learn to build a home or enterprise lab environment where you can safely practice penetration testing techniques and improve your hacking skills, then this book is for you. No prior penetration testing experience is required, as the lab environment is suitable for various skill levels and is used for a wide range of techniques from basic to advance. Whether you are brand new to online learning or you are a seasoned expert, you will be able to set up your own hacking playground depending on your tasks. What You Will Learn Determine your needs and choose the appropriate lab components for them Build a virtual or hardware lab network Imitate an enterprise network and prepare intentionally vulnerable software and services Secure wired and wireless access to your lab Choose a penetration testing framework according to your needs Arm your own wireless hacking platform Get to know the methods to create a strong defense mechanism for your system In Detail Starting with the basics of wireless networking and its associated risks, we will guide you through the stages of creating a penetration testing lab with wireless access and preparing your wireless penetration testing machine. This book will guide you through configuring hardware and virtual network devices, filling the lab network with applications and security solutions, and making it look and work like a real enterprise network. The resulting lab protected with WPA-Enterprise will let you practice most of the attack techniques used in penetration testing projects. Along with a review of penetration testing frameworks, this book is also a detailed manual on preparing a platform for wireless penetration testing. By the end of this book, you will be at the point when you can practice, and research without worrying about your lab environment for every task. Style and approach This is an easy-to-follow guide full of hands-on examples and recipes. Each topic is explained thoroughly and supplies you with the necessary configuration settings. You can pick the recipes you want to follow depending on the task you need to perform.

The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester's Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors. Once you've built your foundation for penetration testing, you’ll learn the Framework's conventions, interfaces, and module system as you launch simulated attacks. You’ll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks. Learn how to: –Find and exploit unmaintained, misconfigured, and unpatched systems –Perform reconnaissance and find valuable information about your target –Bypass anti-virus technologies and circumvent security controls –Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery –Use the Meterpreter shell to launch further attacks from inside the network –Harness standalone Metasploit utilities, third-party tools, and plug-ins –Learn how to write your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to secure your own networks or to put someone else's to the test, Metasploit: The Penetration Tester's Guide will take you there and beyond.

Get started with cybersecurity and progress with the help of expert tips to get certified, find a job, and more Key Features Learn how to follow your desired career path that results in a well-paid, rewarding job in cybersecurity Explore expert tips relating to career paths and certification options Access informative content from a panel of experienced cybersecurity experts Book Description Cybersecurity is an emerging career trend and will continue to become increasingly important. Despite the lucrative pay and significant career growth opportunities, many people are unsure of how to get started. This book is designed by leading industry experts to help you enter the world of cybersecurity with confidence, covering everything from gaining the right certification to tips and tools for finding your first job. The book starts by helping you gain a foundational understanding of cybersecurity, covering cyber law, cyber policy, and frameworks. Next, you'll focus on how to choose the career field best suited to you from options such as security operations, penetration testing, and risk analysis. The book also guides you through the different certification options as well as the pros and cons of a formal college education versus formal certificate courses. Later, you'll discover the importance of defining and understanding your brand. Finally, you'll get up to speed with different career paths and learning opportunities. By the end of this cyber book, you will have gained the knowledge you need to clearly define your career path and develop goals relating to career progression. What you will learn Gain an understanding of cybersecurity essentials, including the different frameworks and laws, and specialties Find out how to land your first job in the cybersecurity industry Understand the difference between college education and certificate courses Build goals and timelines to encourage a work/life balance while delivering value in your job Understand the different types of cybersecurity jobs available and what it means to be entry-level Build affordable, practical labs to develop your technical skills Discover how to set goals and maintain momentum after landing your first cybersecurity job Who this book is for This book is for college graduates, military veterans transitioning from active service, individuals looking to make a mid-career switch, and aspiring IT professionals. Anyone who considers cybersecurity as a potential career field but feels intimidated, overwhelmed, or unsure of where to get started will also find this book useful.

These proceedings represent the work of researchers participating in the 13th International Conference on Cyber Warfare and Security (ICCWS 2018) which is being hosted this year by the National Defense University in Washington DC, USA on 8-9 March 2018.

This book contains selected papers presented at the 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management, held in Maribor, Slovenia, in September 2020.* The 13 full papers included in this volume were carefully reviewed and selected from 21 submissions. Also included is a summary paper of a tutorial. As in previous years, one of the goals of the IFIP Summer School was to encourage the publication of thorough research papers by students and emerging scholars. The papers combine interdisciplinary approaches to bring together a host of perspectives, such as technical, legal, regulatory, socio-economic, social or societal, political, ethical, anthropological, philosophical, or psychological perspectives. *The summer school was held virtually.

Master the art of detecting and averting advanced network security attacks and techniques About This Book Deep dive into the advanced network security attacks and techniques by leveraging tools such as Kali Linux 2, MetaSploit, Nmap, and Wireshark Become an expert in cracking WiFi passwords, penetrating anti-virus networks, sniffing the network, and USB hacks This step-by-step guide shows you how to confidently and quickly detect vulnerabilities for your network before the hacker does Who This Book Is For This book is for network security professionals, cyber security professionals, and Pentesters who are well versed with fundamentals of network security and now want to master it. So whether you're a cyber security professional, hobbyist, business manager, or student aspiring to becoming an ethical hacker or just want to learn more about the cyber security aspect of the IT industry, then this book is definitely for you. What You Will Learn Use SET to clone webpages including the login page Understand the concept of Wi-Fi cracking and use PCAP file to obtain passwords Attack using a USB as payload injector Familiarize yourself with the process of trojan attacks Use Shodan to identify honeypots, rogue access points, vulnerable webcams, and other exploits found in the database Explore various tools for wireless penetration testing and auditing Create an evil twin to intercept network traffic Identify human patterns in networks attacks In Detail Computer networks are increasing at an exponential rate and the most challenging factor organisations are currently facing is network security. Breaching a network is not considered an ingenious effort anymore, so it is very important to gain expertise in securing your network. The book begins by showing you how to identify malicious network behaviour and improve your wireless security. We will teach you what network sniffing is, the various tools associated with it, and how to scan for vulnerable wireless networks. Then we'll show you how attackers hide the payloads and bypass the victim's antivirus. Furthermore, we'll teach you how to spoof IP / MAC address and perform an SQL injection attack and prevent it on your website. We will create an evil twin and demonstrate how to intercept network traffic. Later, you will get familiar with Shodan and Intrusion Detection and will explore the features and tools associated with it. Toward the end, we cover tools such as Yardstick, Ubertooth, Wifi Pineapple, and Alfa used for wireless penetration testing and auditing. This book will show the tools and platform to ethically hack your own network whether it is for your business or for your personal home Wi-Fi. Style and approach This mastering-level guide is for all the security professionals who are eagerly waiting to master network security skills and protecting their organization with ease. It contains practical scenarios on various network security attacks and will teach you how to avert these attacks. This book explains the ongoing war between private business and cyber criminals, state-sponsored attackers, terrorists, and hacktivist groups. Further, it explores the risks posed by trusted employees that put critical information at risk through malice, negligence, or simply making a mistake. It clarifies the historical context of the current situation as it relates to cybersecurity, the challenges facing private business, and the fundamental changes organizations can make to better protect themselves. The problems we face are difficult, but they are not hopeless. Cybercrime continues to grow at an astounding rate. With constant coverage of cyber-attacks in the media, there is no shortage of awareness of increasing threats. Budgets have increased and executives are implementing stronger defenses. Nonetheless, breaches continue to increase in frequency and scope. Building a Comprehensive IT Security Program shares why organizations continue to fail to secure their critical information assets and explains the internal and external adversaries facing organizations today. This book supplies the necessary knowledge and skills to protect organizations better in the future by implementing a comprehensive approach to security. Jeremy Wittkop’s security expertise and critical experience provides insights into topics such as: Who is attempting to steal information and why? What are critical information assets? How are effective programs built? How is stolen information capitalized? How do we shift the paradigm to better protect our organizations? How we can make the cyber world safer for everyone to do business?

The tactical organization and protection of resources is a vital component for any governmental entity. Effectively managing national security through various networks ensures the highest level of protection and defense for citizens and classified information. National Security: Breakthroughs in Research and Practice is an authoritative resource for the latest research on the multiple dimensions of national security, including the political, physical, economic, ecological, and computational dimensions. Highlighting a range of pertinent topics such as data breaches, surveillance, and threat detection, this publication is an ideal reference source for government officials, law enforcement, professionals, researchers, IT professionals, academicians, and graduate-level students seeking current research on the various aspects of national security.

How do the Offensive Security Web Expert results compare with the performance of your competitors and other organizations with similar offerings? What tools and technologies are needed for a custom Offensive Security Web Expert project? What are the success criteria that will indicate that Offensive Security

Web Expert objectives have been met and the benefits delivered? Will team members regularly document their Offensive Security Web Expert work? What problems are you facing and how do you consider Offensive Security Web Expert will circumvent those obstacles? This exclusive Offensive Security Web Expert self-assessment will make you the principal Offensive Security Web Expert domain specialist by revealing just what you need to know to be fluent and ready for any Offensive Security Web Expert challenge. How do I reduce the effort in the Offensive Security Web Expert work to be done to get problems solved? How can I ensure that plans of action include every Offensive Security Web Expert task and that every Offensive Security Web Expert outcome is in place? How will I save time investigating strategic and tactical options and ensuring Offensive Security Web Expert costs are low? How can I deliver tailored Offensive Security Web Expert advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Offensive Security Web Expert essentials are covered, from every angle: the Offensive Security Web Expert self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Offensive Security Web Expert outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Offensive Security Web Expert practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Offensive Security Web Expert are maximized with professional results. Your purchase includes access details to the Offensive Security Web Expert self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book.

How will you know that the Offensive Security project has been successful? How can we improve Offensive Security? How important is Offensive Security to the user organizations mission? What will be the consequences to the stakeholder (financial, reputation etc) if Offensive Security does not go ahead or fails to deliver the objectives? What are the revised rough estimates of the financial savings/opportunity for Offensive Security improvements? This exclusive Offensive Security self-assessment will make you the trusted Offensive Security domain assessor by revealing just what you need to know to be fluent and ready for any Offensive Security challenge. How do I reduce the effort in the Offensive Security work to be done to get problems solved? How can I ensure that plans of action include every Offensive Security task and that every Offensive Security outcome is in place? How will I save time investigating strategic and tactical options and ensuring Offensive Security costs are low? How can I deliver tailored Offensive Security advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Offensive Security essentials are covered, from every angle: the Offensive Security self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Offensive Security outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Offensive Security practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Offensive Security are maximized with professional results. Your purchase includes access details to the Offensive Security self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book. An immersive learning experience enhanced with technical, hands-on labs to understand the concepts, methods, tools, platforms, and systems required to master the art of cybersecurity Key Features Get hold of the best defensive security strategies and tools Develop a defensive security strategy at an enterprise level Get hands-on with advanced cybersecurity threat detection, including XSS, SQL injections, brute forcing web applications, and more Book Description Every organization has its own data and digital assets that need to be protected against an ever-growing threat landscape that compromises the availability, integrity, and confidentiality of crucial data. Therefore, it is important to train professionals in the latest defensive security skills and tools to secure them. Mastering Defensive Security provides you with in-depth knowledge of the latest cybersecurity threats along with the best tools and techniques needed to keep your infrastructure secure. The book begins by establishing a strong foundation of cybersecurity concepts and advances to explore the latest security technologies such as Wireshark, Damn Vulnerable Web App (DVWA), Burp Suite, OpenVAS, and Nmap, hardware threats such as a weaponized Raspberry Pi, and hardening techniques for Unix, Windows, web applications, and cloud infrastructures. As you make progress through the chapters, you'll get to grips with several advanced techniques such as malware analysis, security automation, computer forensics, and vulnerability assessment, which will help you to leverage pentesting for security. By the end of this book, you'll have become familiar with creating your own defensive security tools using IoT devices and developed advanced defensive security skills. What you will learn Become well versed with concepts related to defensive security Discover strategies and tools to secure the most vulnerable factor – the user Get hands-on experience using and configuring the best security tools Understand how to apply hardening techniques in Windows and Unix environments Leverage malware analysis and forensics to enhance your security strategy Secure Internet of Things (IoT) implementations Enhance the security of web applications and cloud deployments Who this book is for This book is for IT professionals, including systems administrators, programmers, IT architects, solution engineers, system analysts, data scientists, DBAs, and any IT expert looking to explore the fascinating world of cybersecurity. Cybersecurity professionals who want to broaden their knowledge of security topics to effectively create and design a defensive security strategy for a large organization will find this book useful. A basic understanding of concepts such as networking, IT, servers, virtualization, and cloud is required.

"Think like our enemy! is a directive straight from Sun Tzu's The Art of War. It is this idea, predating computing by millennia, that is at the core of Red Team Testing. The methodology behind red teaming takes the shackles off of security consultants and pen testers, allowing them to truly test a company's physical, electronic, and computer security. Chris Nickerson details how red team testing provides real world results that can evaluate and drive out business risk in this new age of threats. Security professionals will learn techniques and technologies used by advanced hackers, including how to conduct social. engineering, lock picking, phishing, application, wireless and several more dangerous blended threats. Anyone involved in testing and auditing a company's security must know how where their security is and how to optimize it for today's threats. This book and methodology does just that. Teaches you how to think like a hacker, so that you see security strengths and weaknesses as they truly are Identifies business trick using hacker techniques and tactics like social engineering and blend attacks Provides a methodology for red team testing, including intelligence gathering, planning the attack, and post-compromise reporting

JUMPSTART YOUR NEW AND EXCITING CAREER AS A PENETRATION TESTER The Pentester BluePrint: Your Guide to Being a Pentester offers readers a chance to delve deeply into the world of the ethical, or "white-hat" hacker. Accomplished pentester and author Phillip L. Wylie and cybersecurity researcher Kim Crawley walk you through the basic and advanced topics necessary to understand how to make a career out of finding vulnerabilities in systems, networks, and applications. You'll learn about the role of a penetration tester, what a pentest involves, and the prerequisite knowledge you'll need to start the educational journey of becoming a pentester. Discover how to develop a plan by assessing your current skillset and finding a starting place to begin growing your knowledge and skills. Finally, find out how to become employed as a pentester by using social media, networking strategies, and community involvement. Perfect for IT workers and entry-level information security professionals, The Pentester BluePrint also belongs on the bookshelves of anyone seeking to transition to the exciting and in-demand field of penetration testing. Written in a highly approachable and accessible style, The Pentester BluePrint avoids unnecessarily technical lingo in favor of concrete advice and practical strategies to help you get your start in pentesting. This book will teach you: The foundations of pentesting, including basic IT skills like operating systems, networking, and security systems The development of hacking skills and a hacker mindset Where to find educational options, including college and university classes, security training providers, volunteer work, and self-study Which certifications and degrees are most useful for gaining employment as a pentester How to get experience in the pentesting field, including labs, CTFs, and bug bounties

How do we ensure that implementations of Offensive Security Certified Expert products are done in a way that ensures safety? What potential environmental factors impact the Offensive Security Certified Expert effort? How frequently do you track Offensive Security Certified Expert measures? What sources do you use to gather information for a Offensive Security Certified Expert study? Is the Offensive Security Certified Expert organization completing tasks effectively and efficiently? This premium Offensive Security Certified Expert self-assessment will make you the trusted Offensive Security Certified Expert domain standout by revealing just what you need to know to be fluent and ready for any Offensive Security Certified Expert challenge. How do I reduce the effort in the Offensive Security Certified Expert work to be done to get problems solved? How can I ensure that plans of action include every Offensive Security Certified Expert task and that every Offensive Security Certified Expert outcome is in place? How will I save time investigating strategic and tactical options and ensuring Offensive Security Certified Expert costs are low? How can I deliver tailored Offensive Security Certified Expert advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Offensive Security Certified Expert essentials are covered, from every angle: the Offensive Security Certified Expert self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Offensive Security Certified Expert outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Offensive Security Certified Expert practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Offensive Security Certified Expert are maximized with professional results. Your purchase includes access details to the Offensive Security Certified Expert self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard, and... - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation ...plus an extra, special, resource that helps you with project managing. INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

Who will be responsible for documenting the Offensive Security Certified Professional requirements in detail? How can we incorporate support to ensure safe and effective use of Offensive Security Certified Professional into the services that we provide? How do you assess your Offensive Security Certified Professional workforce capability and capacity needs, including skills, competencies, and staffing levels? Are accountability and ownership for Offensive Security Certified Professional clearly defined? What threat is Offensive Security Certified Professional addressing? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Offensive Security Certified Professional investments work better. This Offensive Security Certified Professional All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Offensive Security Certified Professional Self-Assessment. Featuring 695 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Offensive Security Certified Professional improvements can be made. In using the questions you will be better able to: - diagnose Offensive Security Certified Professional projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in Offensive Security Certified Professional and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the Offensive Security Certified Professional Scorecard, you will develop a clear picture of which Offensive Security Certified Professional areas need attention. Your purchase includes access details to the Offensive Security Certified Professional self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard, and... - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation ...plus an extra, special, resource that helps you with project managing. INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

Use this unique book to leverage technology when conducting offensive security engagements. You will understand practical tradecraft, operational guidelines, and offensive security best practices as carrying out professional cybersecurity engagements is more than exploiting computers, executing scripts, or utilizing tools. Professional Red Teaming introduces you to foundational offensive security concepts. The importance of assessments and ethical hacking is highlighted, and automated assessment technologies are addressed. The state of modern offensive security is discussed in terms of the unique challenges present in professional red teaming. Best practices and operational tradecraft are covered so you feel comfortable in the shaping and carrying out of red team engagements. Anecdotes from actual operations and example scenarios illustrate key concepts and cement a practical understanding of the red team process. You also are introduced to counter advanced persistent threat red teaming (CAPTR teaming). This is a reverse red teaming methodology aimed at specifically addressing the challenges faced from advanced persistent threats (APTs) by the organizations they target and the offensive security professionals trying to mitigate them. What You'll Learn Understand the challenges faced by offensive security assessments Incorporate or conduct red teaming to better mitigate cyber threats Initiate a successful engagement Get introduced to counter-APT red teaming (CAPTR) Evaluate offensive security processes Who This Book Is For Offensive security assessors and those who want a working knowledge of the process, its challenges, and its benefits. Current professionals will gain tradecraft and operational insight and non-technical readers will gain a high-level perspective of what it means to provide and be a customer of red team assessments.

Is there a offensive security kali linux Communication plan covering who needs to get what information when? What is the cause of any offensive security kali linux gaps? What system do you use for gathering offensive security kali linux information? Which individuals, teams or departments will be involved in offensive security kali linux? How can you improve offensive security kali linux? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Offensive Security Kali Linux investments work better. This Offensive Security Kali Linux All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Offensive Security Kali Linux Self-Assessment. Featuring 946 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Offensive Security Kali Linux improvements can be made. In using the questions you will be better able to: - diagnose Offensive Security Kali Linux projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in Offensive Security Kali Linux and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the Offensive Security Kali Linux Scorecard, you will develop a clear picture of which Offensive Security Kali Linux areas need attention. Your purchase includes access details to the Offensive Security Kali Linux self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Offensive Security Kali Linux Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

What are the risks and constraints that you should be concerned about? What other organizational variables, such as reward systems or communication systems, affect the performance of this Offensive Security Certified Professional process? Is there a Offensive Security Certified Professional Communication plan covering who needs to get what information when? Is rapid recovery the most important thing for you? How Does Penetration Testing Relate To Other Life Cycle Products? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are you really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Offensive Security Certified Professional investments work better. This Offensive Security Certified Professional All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Offensive Security Certified Professional Self-Assessment. Featuring 982 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Offensive Security Certified Professional improvements can be made. In using the questions you will be better able to: - diagnose Offensive Security Certified Professional projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in Offensive Security Certified Professional and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the Offensive Security Certified Professional Scorecard, you will develop a clear picture of which Offensive Security Certified Professional areas need attention. Your purchase includes access details to the Offensive Security Certified Professional self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Offensive Security Certified Professional Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

Your ultimate guide to pentesting with Kali Linux Kali is a popular and powerful Linux distribution used by cybersecurity professionals around the world. Penetration testers must master Kali’s varied library of tools to be effective at their work. The Kali Linux Penetration Testing Bible is the hands-on and methodology guide for pentesting with Kali. You’ll discover everything you need to know about the tools and techniques hackers use to gain access to systems like yours so you can erect reliable defenses for your virtual assets. Whether you’re new to the field or an established pentester, you’ll find what you need in this comprehensive guide. Build a modern dockerized environment Discover the fundamentals of the bash language in Linux Use a variety of effective techniques to find vulnerabilities (OSINT, Network Scan, and more) Analyze your findings and identify false positives and uncover advanced subjects, like buffer overflow, lateral movement, and privilege escalation Apply practical and efficient pentesting workflows Learn about Modern Web Application Security Secure SDLC Automate your penetration testing with Python

Expert guidance on the art and science of driving secure behaviors Transformational Security Awareness empowers security leaders with the information and resources they need to assemble and deliver effective world-class security awareness programs that drive secure behaviors and culture change. When all other processes, controls, and technologies fail, humans are your last line of defense. But, how can you prepare them? Frustrated with ineffective training paradigms, most security leaders know that there must be a better way. A way that engages users, shapes behaviors, and fosters an organizational culture that encourages and reinforces security-related values. The good news is that there is hope. That’s what Transformational Security Awareness is all about. Author Perry Carpenter weaves together insights and best practices from experts in communication, persuasion, psychology, behavioral economics, organizational culture management, employee engagement, and storytelling to create a multidisciplinary masterpiece that transcends traditional security education and sets you on the path to make a lasting impact in your organization. Find out what you need to know about marketing, communication, behavior science, and culture management Overcome the knowledge-intention-behavior gap Optimize your program to work with the realities of human nature Use simulations, games, surveys, and leverage new trends like escape rooms to teach security awareness Put effective training together into a well-crafted campaign with ambassadors Understand the keys to sustained success and ongoing culture change Measure your success and establish continuous improvements Do you care more about what your employees know or what they do? It's time to transform the way we think about security awareness. If your organization is stuck in a security awareness rut, using the same ineffective strategies, materials, and information that might check a compliance box but still leaves your organization wide open to phishing, social engineering, and security-related employee mistakes and oversights, then you NEED this book.

The Basics of Web Hacking introduces you to a tool-driven process to identify the most widespread vulnerabilities in Web applications. No prior experience is needed. Web apps are a "path of least resistance" that can be exploited to cause the most damage to a system, with the lowest hurdles to overcome. This is a perfect storm for beginning hackers. The process set forth in this book introduces not only the theory and practical information related to these vulnerabilities, but also the detailed configuration and usage of widely available tools necessary to exploit these vulnerabilities. The Basics of Web Hacking provides a simple and clean explanation of how to utilize tools such as Burp Suite, sqlmap, and Zed Attack Proxy (ZAP), as well as basic network scanning tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more. Dr. Josh Pauli teaches software security at Dakota State University and has presented on this topic to the U.S. Department of Homeland Security, the NSA, BlackHat Briefings, and Defcon. He will lead you through a focused, three-part approach to Web security, including hacking the server, hacking the Web app, and hacking the Web user. With Dr. Pauli’s approach, you will fully understand the what/where/why/how of the most widespread Web vulnerabilities and how easily they can be exploited with the correct tools. You will learn how to set up a safe environment to conduct these attacks, including an attacker Virtual Machine (VM) with all necessary tools and several known-vulnerable Web application VMs that are widely available and maintained for this very purpose. Once you complete the entire process, not only will you be prepared to test for the most damaging Web exploits, you will also be prepared to conduct more advanced Web hacks that mandate a strong base of knowledge. Provides a simple and clean approach to Web hacking, including hands-on examples and exercises that are designed to teach you how to hack the server, hack the Web app, and hack the Web user Covers the most significant new tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more! Written by an author who works in the field as a penetration tester and who teaches Web security classes at Dakota State University

Is your enterprise flexible and adaptable while using the SWG? How does the Security Gateway support correlation for end-to-end transaction logging? What percentage of staff had security training last year? Are you aware of anyone attempting to gain information in person, by phone, mail, email, etc., regarding the configuration and/or cyber security posture of your website, network, software, or hardware? When do you have to generate new licenses? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Offensive Security Web Expert investments work better. This Offensive Security Web Expert All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Offensive Security Web Expert Self-Assessment. Featuring 976 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Offensive Security Web Expert improvements can be made. In using the questions you will be better able to: - diagnose Offensive Security Web Expert projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in Offensive Security Web Expert and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the Offensive Security Web Expert Scorecard, you will develop a clear picture of which Offensive Security Web Expert areas need attention. Your purchase includes access details to the Offensive Security Web Expert self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Offensive Security Web Expert Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.