

Network Penetration Testing Training

CompTIA PenTest+ Certification All-in-One Exam Guide (Exam PT0-001)
 Penetration Testing Basics
 Mastering Modern Web Penetration Testing
 Practical Web Penetration Testing
 Mastering Kali Linux for Advanced Penetration Testing
 BackTrack 4
 Advanced Penetration Testing
 Building Virtual Pentesting Labs for Advanced Penetration Testing
 Web Penetration Testing with Kali Linux
 Social Engineering Penetration Testing
 Backtrack 5 Wireless Penetration Testing
 The Basics of Hacking and Penetration Testing
 Learning Penetration Testing with Python
 Hands-On Penetration Testing with Kali NetHunter
 The Art of Network Penetration Testing
 CEH Certified Ethical Hacker All-in-One Exam Guide, Fifth Edition
 Penetration Testing Essential Training
 Penetration Tester's Open Source Toolkit
 The Network Security Test Lab
 Penetration Testing and Network Defense
 Unauthorised Access
 Penetration Testing Essentials
 The Pentester BluePrint
 Learning Pentesting for Android Devices
 Professional Penetration Testing
 Kali Linux Wireless Penetration Testing: Beginner's Guide
 CEH: Certified Ethical Hacker Version 8 Study Guide
 Metasploit Revealed: Secrets of the Expert Pentester
 CompTIA PenTest+ Certification For Dummies
 Learning Kali Linux
 Python: Penetration Testing for Developers
 Certified Ethical Hacker (CEH) Version 9 Cert Guide
 Learn Ethical Hacking from Scratch
 Professional Penetration Testing
 Hacking and Penetration Testing with Low Power Devices
 CompTIA PenTest+ Certification Passport (Exam PT0-001)
 Certified Ethical Hacker (CEH) Foundation Guide
 Advanced Penetration Testing for Highly-Secured Environments
 Penetration Testing

Network Penetration Testing Training

Downloaded from dev.mabts.edu by guest

MAXIMILLIAN BRENNAN

[CompTIA PenTest+ Certification All-in-One Exam Guide \(Exam PT0-001\)](#) John Wiley & Sons
 Master the art of penetration testing with BackTrack.

[Penetration Testing Basics](#) Packt Publishing Ltd

This is an easy-to-follow guide, full of hands-on and real-world examples of applications. Each of the vulnerabilities discussed in the book is accompanied with the practical approach to the vulnerability, and the underlying security issue. This book is intended for all those who are looking to get started in Android security or Android application penetration testing. You don't need to be an Android developer to learn from this book, but it is highly recommended that developers have some experience in order to learn how to create secure applications for Android.

[Mastering Modern Web Penetration Testing](#) Elsevier

Web Applications are the core of any business today, and the need for specialized Application Security experts is increasing these days. Using this book, you will be able to learn Application Security testing and understand how to analyze a web application, conduct a web intrusion test, and a network infrastructure test.

Syngress Press

This effective self-study guide serves as an accelerated review of all exam objectives for the CompTIA PenTest+ certification exam This concise, quick-review test preparation guide offers 100% coverage of all exam objectives for the new CompTIA PenTest+ exam. Designed as an accelerated review of all the key information covered on the exam, the Passport's established pedagogy enables you to tailor a course for study and drill down into the exam objectives. Special elements highlight actual exam topics and point you to additional resources for further information. Written by an IT security expert and experienced author, CompTIA PenTest+ Certification Passport (Exam PT0-001) focuses on exactly what you need to know to pass the exam. The book features end of chapter review sections that provide bulleted summations organized by exam objective. Accurate practice exam questions with in-depth answer explanations aid in retention, reinforce what you have learned, and show how this information directly relates to the exam. • Online content includes access to the TotalTester online test engine with 200 multiple-choice practice questions and additional performance-based questions • Follows the newly-refreshed Certification Passport series developed by training guru Mike Meyers • Includes a 10% off exam voucher coupon, a \$35 value

[Practical Web Penetration Testing](#) Apress

The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. Summary Penetration testing is about more than just getting through a perimeter firewall. The biggest security threats are inside the network, where attackers can rampage through sensitive data by exploiting weak access controls and poorly patched software. Designed for up-and-coming security professionals, The Art of Network Penetration Testing teaches you how to take over an enterprise network from the inside. It lays out every stage of an internal security assessment step-by-step, showing you how to identify weaknesses before a malicious invader can do real damage. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Penetration testers uncover security gaps by attacking networks exactly like malicious intruders do. To become a world-class pentester, you need to master offensive security concepts, leverage a proven methodology, and practice, practice, practice. This book delivers insights from security expert Royce Davis, along with a virtual testing environment you can use to hone your skills. About the book The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from

information gathering to seizing control of a system and owning the network. As you brute force passwords, exploit unpatched services, and elevate network level privileges, you'll learn where the weaknesses are—and how to take advantage of them. What's inside Set up a virtual pentest lab Exploit Windows and Linux network vulnerabilities Establish persistent re-entry to compromised targets Detail your findings in an engagement report About the reader For tech professionals. No security experience required. About the author Royce Davis has orchestrated hundreds of penetration tests, helping to secure many of the largest companies in the world. Table of Contents 1 Network Penetration Testing PHASE 1 - INFORMATION GATHERING 2 Discovering network hosts 3 Discovering network services 4 Discovering network vulnerabilities PHASE 2 - FOCUSED PENETRATION 5 Attacking vulnerable web services 6 Attacking vulnerable database services 7 Attacking unpatched services PHASE 3 - POST-EXPLOITATION AND PRIVILEGE ESCALATION 8 Windows post-exploitation 9 Linux or UNIX post-exploitation 10 Controlling the entire network PHASE 4 - DOCUMENTATION 11 Post-engagement cleanup 12 Writing a solid pentest deliverable [Mastering Kali Linux for Advanced Penetration Testing](#) John Wiley & Sons Advance your existing career, or build a new one, with the PenTest+ certification Looking for some hands-on help achieving one of the tech industry's leading new certifications? Complete with an online test bank to help you prep for the exam, CompTIA PenTest+ Certification For Dummies, 2nd Edition guides you through every competency tested by the exam. Whether you're a seasoned security pro looking to add a new cert to your skillset, or you're an early-career cybersecurity professional seeking to move forward, you'll find the practical, study-centered guidance you need to succeed on the certification exam. In this book and online, you'll get: A thorough introduction to the planning and information gathering phase of penetration testing, including scoping and vulnerability identification Comprehensive examinations of system exploits, vulnerabilities in wireless networks, and app-based intrusions In-depth descriptions of the PenTest+ exam and an Exam Reference Matrix to help you get more familiar with the structure of the test Three practice tests online with questions covering every competency on the exam Perfect for cybersecurity pros looking to add an essential new certification to their repertoire, CompTIA PenTest+ Certification For Dummies, 2nd Edition is also a great resource for those looking for a way to cement and build on fundamental pentesting skills.

BackTrack 4 Simon and Schuster

Master the art of conducting modern pen testing attacks and techniques on your web application before the hacker does! About This Book This book covers the latest technologies such as Advance XSS, XSRF, SQL Injection, Web API testing, XML attack vectors, OAuth 2.0 Security, and more involved in today's web applications Penetrate and secure your web application using various techniques Get this comprehensive reference guide that provides advanced tricks and tools of the trade for seasoned penetration testers Who This Book Is For This book is for security professionals and penetration testers who want to speed up their modern web application penetrating testing. It will also benefit those at an intermediate level and web developers who need to be aware of the latest application hacking techniques. What You Will Learn Get to know the new and less-publicized techniques such PHP Object Injection and XML-based vectors Work with different security tools to automate most of the redundant tasks See different kinds of newly-designed security headers and how they help to provide security Exploit and detect different kinds of XSS vulnerabilities Protect your web application using filtering mechanisms Understand old school and classic web hacking in depth using SQL Injection, XSS, and CSRF Grasp XML-related vulnerabilities and attack vectors such as XXE and DoS techniques Get to know how to test REST APIs to discover security issues in them In Detail Web penetration testing is a growing, fast-moving, and absolutely critical field in information security. This book executes modern web application attacks and utilises cutting-edge hacking techniques with an enhanced knowledge of web application security. We will cover web hacking techniques so you can explore the attack vectors during penetration tests. The book encompasses

the latest technologies such as OAuth 2.0, Web API testing methodologies and XML vectors used by hackers. Some lesser discussed attack vectors such as RPO (relative path overwrite), DOM clobbering, PHP Object Injection and etc. has been covered in this book. We'll explain various old school techniques in depth such as XSS, CSRF, SQL Injection through the ever-dependable SQLMap and reconnaissance. Websites nowadays provide APIs to allow integration with third party applications, thereby exposing a lot of attack surface, we cover testing of these APIs using real-life examples. This pragmatic guide will be a great benefit and will help you prepare fully secure applications. Style and approach This master-level guide covers various techniques serially. It is power-packed with real-world examples that focus more on the practical aspects of implementing the techniques rather going into detailed theory.

Advanced Penetration Testing John Wiley & Sons

Exploit the secrets of Metasploit to master the art of penetration testing. About This Book Discover techniques to integrate Metasploit with the industry's leading tools Carry out penetration testing in highly-secured environments with Metasploit and acquire skills to build your defense against organized and complex attacks Using the Metasploit framework, develop exploits and generate modules for a variety of real-world scenarios Who This Book Is For This course is for penetration testers, ethical hackers, and security professionals who'd like to master the Metasploit framework and explore approaches to carrying out advanced penetration testing to build highly secure networks. Some familiarity with networking and security concepts is expected, although no familiarity of Metasploit is required. What You Will Learn Get to know the absolute basics of the Metasploit framework so you have a strong foundation for advanced attacks Integrate and use various supporting tools to make Metasploit even more powerful and precise Test services such as databases, SCADA, and many more Attack the client side with highly advanced techniques Test mobile and tablet devices with Metasploit Understand how to Customize Metasploit modules and modify existing exploits Write simple yet powerful Metasploit automation scripts Explore steps involved in post-exploitation on Android and mobile platforms In Detail Metasploit is a popular penetration testing framework that has one of the largest exploit databases around. This book will show you exactly how to prepare yourself against the attacks you will face every day by simulating real-world possibilities. This learning path will begin by introducing you to Metasploit and its functionalities. You will learn how to set up and configure Metasploit on various platforms to create a virtual test environment. You will also get your hands on various tools and components and get hands-on experience with carrying out client-side attacks. In the next part of this learning path, you'll develop the ability to perform testing on various services such as SCADA, databases, IoT, mobile, tablets, and many more services. After this training, we jump into real-world sophisticated scenarios where performing penetration tests are a challenge. With real-life case studies, we take you on a journey through client-side attacks using Metasploit and various scripts built on the Metasploit framework. The final instalment of your learning journey will be covered through a bootcamp approach. You will be able to bring together the learning together and speed up and integrate Metasploit with leading industry tools for penetration testing. You'll finish by working on challenges based on user's preparation and work towards solving the challenge. The course provides you with highly practical content explaining Metasploit from the following Packt books: Metasploit for Beginners Mastering Metasploit, Second Edition Metasploit Bootcamp Style and approach This pragmatic learning path is packed with start-to-end instructions from getting started with Metasploit to effectively building new things and solving real-world examples. All the key concepts are explained with the help of examples and demonstrations that will help you understand everything to use this essential IT power tool.

Building Virtual Pentesting Labs for Advanced Penetration Testing CompTIA PenTest+ Certification All-in-One Exam Guide (Exam PT0-001)

Unleash the power of Python scripting to execute effective and efficient penetration tests About This Book Sharpen your pentesting skills with Python Develop your fluency with Python to write sharper scripts for rigorous security testing Get stuck into some of the most powerful tools in the security world Who This Book Is For If you are a Python programmer or a security researcher who has basic knowledge of Python programming and wants to learn about penetration testing with the help of Python, this course is ideal for you. Even if you are new to the field of ethical hacking, this course can help you find the vulnerabilities in your system so that you are ready to tackle any kind of attack or intrusion. What You Will Learn Familiarize yourself with the generation of Metasploit resource files and use the Metasploit Remote Procedure Call to automate exploit generation and execution Exploit the Remote File Inclusion to gain administrative access to systems with Python and other scripting languages Crack an organization's Internet perimeter and chain exploits to gain deeper access to an organization's resources Explore wireless traffic with the help of various programs and perform wireless attacks with Python programs Gather passive information from a website using automated scripts and perform XSS, SQL injection, and parameter tampering attacks Develop complicated header-based attacks through Python In Detail Cybercriminals are always one step ahead, when it comes to tools and techniques. This means you need to use the same tools and adopt the same mindset to properly secure your software. This course shows you how to do just that, demonstrating how effective Python can be for powerful pentesting that keeps your software safe. Comprising of three key modules, follow each one to push your Python and security skills to the next level. In the first module, we'll show you how to get to grips with the fundamentals. This means you'll quickly find out how to tackle some of the common challenges facing pentesters using custom Python tools designed specifically for your needs. You'll also learn what tools to use and when, giving you complete confidence when deploying your pentester tools to combat any potential threat. In the next module you'll begin hacking into the application layer. Covering everything from parameter tampering, DDoS, XSS, and SQL injection, it will build on the knowledge and skills you learned in the first module to make you an even more fluent security expert. Finally in the third module, you'll find more than 60 Python pentesting recipes. We think this will soon become your trusted resource for any pentesting situation. This Learning Path combines some of the best that Packt has to offer in one complete, curated package. It includes content from the following Packt products: Learning Penetration Testing with Python by Christopher Duffy Python Penetration Testing Essentials by Mohit Python Web Penetration Testing Cookbook by Cameron Buchanan, Terry Ip, Andrew Mabbitt, Benjamin May and Dave Mound Style and approach This course provides a quick access to powerful, modern tools, and customizable scripts to kick-start the creation of your own Python web penetration testing toolbox.

Web Penetration Testing with Kali Linux John Wiley & Sons

This is the eBook edition of the Certified Ethical Hacker (CEH) Version 9 Cert Guide. This eBook does not include the practice exam that comes with the print edition. In this best-of-breed study guide, Certified Ethical Hacker (CEH) Version 9 Cert Guide, leading expert Michael Gregg helps you master all the topics you need to know to succeed on your Certified Ethical Hacker Version 9 exam and advance your career in IT security. Michael's concise, focused approach explains every exam objective from a real-world perspective, helping you quickly identify weaknesses and retain everything you need to know. Every feature of this book is designed to support both efficient exam preparation and long-term mastery: · Opening Topics Lists identify the topics you need to learn in each chapter and list EC-Council's official exam objectives · Key Topics figures, tables, and lists call

attention to the information that's most crucial for exam success · Exam Preparation Tasks enable you to review key topics, complete memory tables, define key terms, work through scenarios, and answer review questions...going beyond mere facts to master the concepts that are crucial to passing the exam and enhancing your career · Key Terms are listed in each chapter and defined in a complete glossary, explaining all the field's essential terminology This study guide helps you master all the topics on the latest CEH exam, including · Ethical hacking basics · Technical foundations of hacking · Footprinting and scanning · Enumeration and system hacking · Linux distro's, such as Kali and automated assessment tools · Trojans and backdoors · Sniffers, session hijacking, and denial of service · Web server hacking, web applications, and database attacks · Wireless technologies, mobile security, and mobile attacks · IDS, firewalls, and honeypots · Buffer overflows, viruses, and worms · Cryptographic attacks and defenses · Cloud security and social engineering

Social Engineering Penetration Testing John Wiley & Sons

This comprehensive exam guide offers 100% coverage of every topic on the CompTIA PenTest+ exam Get complete coverage of all the objectives included on the CompTIA PenTest+ certification exam PT0-001 from this comprehensive resource. Written by an expert penetration tester, the book provides learning objectives at the beginning of each chapter, hands-on exercises, exam tips, and practice questions with in-depth answer explanations. Designed to help you pass the exam with ease, this definitive volume also serves as an essential on-the-job reference. Covers all exam topics, including: ·Pre-engagement activities ·Getting to know your targets ·Network scanning and enumeration ·Vulnerability scanning and analysis ·Mobile device and application testing ·Social engineering ·Network-based attacks ·Wireless and RF attacks ·Web and database attacks ·Attacking local operating systems ·Physical penetration testing ·Writing the pen test report ·And more Online content includes: ·Interactive performance-based questions ·Test engine that provides full-length practice exams or customized quizzes by chapter or by exam domain

Backtrack 5 Wireless Penetration Testing Packt Publishing Ltd

Social engineering attacks target the weakest link in an organization's security human beings. Everyone knows these attacks are effective, and everyone knows they are on the rise. Now, Social Engineering Penetration Testing gives you the practical methodology and everything you need to plan and execute a social engineering penetration test and assessment. You will gain fascinating insights into how social engineering techniques including email phishing, telephone pretexting, and physical vectors can be used to elicit information or manipulate individuals into performing actions that may aid in an attack. Using the book's easy-to-understand models and examples, you will have a much better understanding of how best to defend against these attacks. The authors of Social Engineering Penetration Testing show you hands-on techniques they have used at RandomStorm to provide clients with valuable results that make a real difference to the security of their businesses. You will learn about the differences between social engineering pen tests lasting anywhere from a few days to several months. The book shows you how to use widely available open-source tools to conduct your pen tests, then walks you through the practical steps to improve defense measures in response to test results. Understand how to plan and execute an effective social engineering assessment Learn how to configure and use the open-source tools available for the social engineer Identify parts of an assessment that will most benefit time-critical engagements Learn how to design target scenarios, create plausible attack situations, and support various attack vectors with technology Create an assessment report, then improve defense measures in response to test results

The Basics of Hacking and Penetration Testing Pearson IT Certification

Hacking and Penetration Testing with Low Power Devices shows you how to perform penetration tests using small, low-powered devices that are easily hidden and may be battery-powered. It shows how to use an army of devices, costing less than you might spend on a laptop, from distances of a mile or more. Hacking and Penetration Testing with Low Power Devices shows how to use devices running a version of The Deck, a full-featured penetration testing and forensics Linux distribution, and can run for days or weeks on batteries due to their low power consumption. Author Philip Polstra shows how to use various configurations, including a device the size of a deck of cards that can easily be attached to the back of a computer. While each device running The Deck is a full-featured pen-testing platform, connecting systems together via 802.15.3 networking gives you even more power and flexibility. This reference teaches you how to construct and power these devices, install operating systems, and fill out your toolbox of small low-power devices with hundreds of tools and scripts from the book's companion website. Hacking and Pen Testing with Low Power Devices puts all these tools into your hands and will help keep you at the top of your game performing cutting-edge pen tests from anywhere in the world! Understand how to plan and execute an effective penetration test using an army of low-power devices Learn how to configure and use open-source tools and easy-to-construct low-power devices Leverage IEEE 802.15.4 networking to perform penetration tests from up to a mile away, or use 802.15.4 gateways to perform pen tests from anywhere in the world Access penetration testing operating systems with hundreds of tools and scripts on the book's companion web site

Learning Penetration Testing with Python Packt Publishing Ltd

With more than 600 security tools in its arsenal, the Kali Linux distribution can be overwhelming. Experienced and aspiring security professionals alike may find it challenging to select the most appropriate tool for conducting a given test. This practical book covers Kali's expansive security capabilities and helps you identify the tools you need to conduct a wide range of security tests and penetration tests. You'll also explore the vulnerabilities that make those tests necessary. Author Ric Messier takes you through the foundations of Kali Linux and explains methods for conducting tests on networks, web applications, wireless security, password vulnerability, and more. You'll discover different techniques for extending Kali tools and creating your own toolset. Learn tools for stress testing network stacks and applications Perform network reconnaissance to determine what's available to attackers Execute penetration tests using automated exploit tools such as Metasploit Use cracking tools to see if passwords meet complexity requirements Test wireless capabilities by injecting frames and cracking passwords Assess web application vulnerabilities with automated or proxy-based tools Create advanced attack techniques by extending Kali tools or developing your own Use Kali Linux to generate reports once testing is complete

Hands-On Penetration Testing with Kali NetHunter Newnes

Wireless has become ubiquitous in today's world. The mobility and flexibility provided by it makes our lives more comfortable and productive. But this comes at a cost - Wireless technologies are inherently insecure and can be easily broken. BackTrack is a penetration testing and security auditing distribution that comes with a myriad of wireless networking tools used to simulate network attacks and detect security loopholes. Backtrack 5 Wireless Penetration Testing Beginner's Guide will take you through the journey of becoming a Wireless hacker. You will learn various wireless testing methodologies taught using live examples, which you will implement throughout this book. The engaging practical sessions very gradually grow in complexity giving you enough time to ramp up before you get to advanced wireless attacks. This book will take you through the basic concepts in Wireless and creating a lab environment for your experiments to the business of different lab sessions in wireless security basics, slowly turn on the heat and move to more complicated scenarios, and finally end your journey by conducting bleeding edge wireless attacks in your lab. There are many interesting and new things that you will learn in this book - War Driving, WLAN

packet sniffing, Network Scanning, Circumventing hidden SSIDs and MAC filters, bypassing Shared Authentication, Cracking WEP and WPA/WPA2 encryption, Access Point MAC spoofing, Rogue Devices, Evil Twins, Denial of Service attacks, Viral SSIDs, Honeytrap and Hotspot attacks, Caffe Latte WEP Attack, Man-in-the-Middle attacks, Evading Wireless Intrusion Prevention systems and a bunch of other cutting edge wireless attacks. If you were ever curious about what wireless security and hacking was all about, then this book will get you started by providing you with the knowledge and practical know-how to become a wireless hacker. Hands-on practical guide with a step-by-step approach to help you get started immediately with Wireless Penetration Testing

The Art of Network Penetration Testing Packt Publishing Ltd

Continuing a tradition of excellent training on open source tools, Penetration Tester's Open Source Toolkit, Fourth Edition is a great reference to the open source tools available today and teaches you how to use them by demonstrating them in real-world examples. This book expands upon existing documentation so that a professional can get the most accurate and in-depth test results possible. Real-life scenarios are a major focus so that the reader knows which tool to use and how to use it for a variety of situations. This updated edition covers the latest technologies and attack vectors, including industry specific case studies and complete laboratory setup. Great commercial penetration testing tools can be very expensive and sometimes hard to use or of questionable accuracy. This book helps solve both of these problems. The open source, no-cost penetration testing tools presented work as well or better than commercial tools and can be modified by the user for each situation if needed. Many tools, even ones that cost thousands of dollars, do not come with any type of instruction on how and in which situations the penetration tester can best use them. Penetration Tester's Open Source Toolkit, Fourth Edition bridges this gap providing the critical information that you need. Details current open source penetration tools Presents core technologies for each type of testing and the best tools for the job New to this edition: expanded wireless pen testing coverage to include Bluetooth, coverage of cloud computing and virtualization, new tools, and the latest updates to tools, operating systems, and techniques Includes detailed laboratory environment setup, new real-world examples, and industry-specific case studies

CEH Certified Ethical Hacker All-in-One Exam Guide, Fifth Edition McGraw Hill Professional

Professional Penetration Testing walks you through the entire process of setting up and running a pen test lab. Penetration testing—the act of testing a computer network to find security vulnerabilities before they are maliciously exploited—is a crucial component of information security in any organization. With this book, you will find out how to turn hacking skills into a professional career. Chapters cover planning, metrics, and methodologies; the details of running a pen test, including identifying and verifying vulnerabilities; and archiving, reporting and management practices. Author Thomas Wilhelm has delivered penetration testing training to countless security professionals, and now through the pages of this book you can benefit from his years of experience as a professional penetration tester and educator. After reading this book, you will be able to create a personal penetration test lab that can deal with real-world vulnerability scenarios. All disc-based content for this title is now available on the Web. Find out how to turn hacking and pen testing skills into a professional career Understand how to conduct controlled attacks on a network through real-world examples of vulnerable and exploitable servers Master project management skills necessary for running a formal penetration test and setting up a professional ethical hacking business Discover metrics and reporting methodologies that provide experience crucial to a professional penetration tester

Penetration Testing Essential Training John Wiley & Sons

Your pen testing career begins here, with a solid foundation in essential skills and concepts Penetration Testing Essentials provides a starting place for professionals and beginners looking to learn more about penetration testing for cybersecurity. Certification eligibility requires work experience—but before you get that experience, you need a basic understanding of the technical and behavioral ways attackers compromise security, and the tools and techniques you'll use to discover the weak spots before others do. You'll learn information gathering techniques, scanning and enumeration, how to target wireless networks, and much more as you build your pen tester skill set. You'll learn how to break in, look around, get out, and cover your tracks, all without ever being noticed. Pen testers are tremendously important to data security, so they need to be sharp and well-versed in technique, but they also need to work smarter than the average hacker. This book set you on the right path, with expert instruction from a veteran IT security expert with multiple security certifications. IT Security certifications have stringent requirements and demand a complex body of

knowledge. This book lays the groundwork for any IT professional hoping to move into a cybersecurity career by developing a robust pen tester skill set. Learn the fundamentals of security and cryptography Master breaking, entering, and maintaining access to a system Escape and evade detection while covering your tracks Build your pen testing lab and the essential toolbox Start developing the tools and mindset you need to become experienced in pen testing today.

Penetration Tester's Open Source Toolkit Syngress

Build a better defense against motivated, organized, professional attacks Advanced Penetration Testing: Hacking the World's Most Secure Networks takes hacking far beyond Kali linux and Metasploit to provide a more complex attack simulation. Featuring techniques not taught in any certification prep or covered by common defensive scanners, this book integrates social engineering, programming, and vulnerability exploits into a multidisciplinary approach for targeting and compromising high security environments. From discovering and creating attack vectors, and moving unseen through a target enterprise, to establishing command and exfiltrating data—even from organizations without a direct Internet connection—this guide contains the crucial techniques that provide a more accurate picture of your system's defense. Custom coding examples use VBA, Windows Scripting Host, C, Java, JavaScript, Flash, and more, with coverage of standard library applications and the use of scanning tools to bypass common defensive measures. Typical penetration testing 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. The professional hackers and nation states on the forefront of today's threats operate at a much more complex level—and this book shows you how to defend your high security network. Use targeted social engineering pretexts to create the initial compromise Leave a command and control structure in place for long-term access Escalate privilege and breach networks, operating systems, and trust structures Infiltrate further using harvested credentials while expanding control Today's threats are organized, professionally-run, and very much for-profit. Financial institutions, health care organizations, law enforcement, government agencies, and other high-value targets need to harden their IT infrastructure and human capital against targeted advanced attacks from motivated professionals. Advanced Penetration Testing goes beyond Kali linux and Metasploit and to provide you advanced pen testing for high security networks.

The Network Security Test Lab Syngress

The practical guide to simulating, detecting, and responding to network attacks Create step-by-step testing plans Learn to perform social engineering and host reconnaissance Evaluate session hijacking methods Exploit web server vulnerabilities Detect attempts to breach database security Use password crackers to obtain access information Circumvent Intrusion Prevention Systems (IPS) and firewall protections and disrupt the service of routers and switches Scan and penetrate wireless networks Understand the inner workings of Trojan Horses, viruses, and other backdoor applications Test UNIX, Microsoft, and Novell servers for vulnerabilities Learn the root cause of buffer overflows and how to prevent them Perform and prevent Denial of Service attacks Penetration testing is a growing field but there has yet to be a definitive resource that instructs ethical hackers on how to perform a penetration test with the ethics and responsibilities of testing in mind. Penetration Testing and Network Defense offers detailed steps on how to emulate an outside attacker in order to assess the security of a network. Unlike other books on hacking, this book is specifically geared towards penetration testing. It includes important information about liability issues and ethics as well as procedures and documentation. Using popular open-source and commercial applications, the book shows you how to perform a penetration test on an organization's network, from creating a test plan to performing social engineering and host reconnaissance to performing simulated attacks on both wired and wireless networks. Penetration Testing and Network Defense also goes a step further than other books on hacking, as it demonstrates how to detect an attack on a live network. By detailing the method of an attack and how to spot an attack on your network, this book better prepares you to guard against hackers. You will learn how to configure, record, and thwart these attacks and how to harden a system to protect it against future internal and external attacks. Full of real-world examples and step-by-step procedures, this book is both an enjoyable read and full of practical advice that will help you assess network security and develop a plan for locking down sensitive data and company resources. "This book goes to great lengths to explain the various testing approaches that are used today and gives excellent insight into how a responsible penetration testing specialist executes his trade." -Bruce Murphy, Vice President, World Wide Security Services, Cisco Systems(R)

Related with Network Penetration Testing Training:

© [Network Penetration Testing Training Utah Business Economic Outlook Summit](#)

© [Network Penetration Testing Training Utopia Guide Long Iskand](#)

© [Network Penetration Testing Training Uss Kitty Hawk Deployment History](#)