Ethical Hacking And Penetration Testing Guide

Learn Ethical Hacking from Scratch
Penetration Testing
Ethical Hacking for Beginners
Penetration Testing For Dummies
The Basics of Hacking and Penetration Testing
The Basics of Hacking and Penetration Testing
Ethical Hacking: The Ultimate Guide to Using Penetration Testing to Audit and Improve the Cybersecurity of Computer Networks for Beginn
Penetration Testing Azure for Ethical Hackers
Ethical Hacker's Certification Guide (CEHv11)
Hands on Hacking
The Ethical Hack
Certified Ethical Hacker (CEH) Preparation Guide
Python Ethical Hacking from Scratch
Infrastructure Attack Strategies for Ethical Hacking
Kali Linux - An Ethical Hacker's Cookbook
The Pentester BluePrint
The New Penetrating Testing for Beginners
Learning Kali Linux
Web Penetration Testing with Kali Linux
Ethical Hacking and Penetration Testing Guide
Ethical Hacking: Penetration Testing

Hacking For Beginners
The Ultimate Kali Linux Book
Ethical Hacking
Perspectives on Ethical Hacking and Penetration Testing
Ethical Hacking
ETHICAL HACKING FOR BEGINNERS
Hacking and Penetration Testing with Low Power Devices
The Advanced Penetrating Testing
Advanced Penetration Testing
Linux Basics for Hackers
Mastering Kali Linux for Advanced Penetration Testing
Hacking Essentials
Hacking
The Basics of Hacking and Penetration Testing
The Hacker Ethos
Python for Offensive PenTest
Python Penetration Testing Essentials
Ethical Hacking and Penetration, Step by Step with Kali Linux
Professional Penetration Testing

INGRID FINN

Learn Ethical Hacking from Scratch CRC Press Have you always been curious about hacking? Have you also had a misconception about the term Ethical Hacking? Would you like to learn more about ethical hacking using a powerful

operating system called Kali Linux? Do you aspire to start an ethical hacking career someday? Then this is the right book to help you get started. This book will prove to be a valuable source of knowledge, especially when you want to learn a lot about ethical hacking in a short amount of time. This treasure trove of knowledge will teach you about the power of Kali Linux and how its tools can help you during every stage of the penetration testing lifecycle. If you want to launch yourself into the world of ethical hacking and want to use Kali Linux as the most used tool in your toolkit, this book will definitely serve as your launchpad. The book is designed to consider first time Kali Linux users and will take you through a step by step guide on how to download and install Kali Linux. The book is also designed to help existing Kali Linux users learn advanced techniques concerning the use of Kali Linux in the penetration testing lifecycle and the ethical hacking domain. The tools surrounding the Kali Linux operating system in this course will help you get a first impression of the ethical hacking profile and will also serve as a platform to

launch you into the world of information security. The book will take you through: An overview of hacking Terminologies of hacking Steps to download and install Kali Linux The penetration testing lifecycle Dedicated chapters on the five stages of the penetration testing lifecycle viz. Reconnaissance, Scanning, Exploitation, Maintaining Access, and Reporting And a bonus chapter on Email Hacking The book has been designed for you to understand hacking and Kali Linux from its foundation. You will not need to complete the entire book to start with a practical performance on Kali Linux. Every chapter of the penetration testing life cycle is a module in itself, and you will be in a position to try out the tools listed in them as you finish each chapter. There are step-by-step instructions and code snippets throughout the book that will help you get your hands dirty on a real Kali Linux system with the completion of each chapter. So here's hoping that this book helps you find the appetite to become an ethical hacker someday soon! Click the Buy Now button to get started now. **Penetration Testing** Packt Publishing Ltd Originally, the term “hacker” referred to a programmer

who was skilled in computer operating systems and machine code. Today, it refers to anyone who performs hacking activities. Hacking is the act of changing a system's features to attain a goal that is not within the original purpose of the creator. The word "hacking" is usually perceived negatively especially by people who do not understand the job of an ethical hacker. In the hacking world, ethical hackers are good guys. What is their role? They use their vast knowledge of computers for good instead of malicious reasons. They look for vulnerabilities in the computer security of organizations and businesses to prevent bad actors from taking advantage of them. For someone that loves the world of technology and computers, it would be wise to consider an ethical hacking career. You get paid (a good amount) to break into systems. Getting started will not be a walk in the park—just as with any other career. However, if you are determined, you can skyrocket yourself into a lucrative career. When you decide to get started on this journey, you will have to cultivate patience. The first step for

many people is usually to get a degree in computer science. You can also get an A+ certification (CompTIA)—you must take and clear two different exams. To be able to take the qualification test, you need to have not less than 500 hours of experience in practical computing. Experience is required, and a CCNA or Network+ qualification to advance your career.

Ethical Hacking for Beginners

John Wiley & Sons

Explore the world of practical ethical hacking by developing custom network scanning and remote access tools that will help you test the system security of your organization Key Features Get hands-on with ethical hacking and learn to think like a real-life hacker Build practical ethical hacking tools from scratch with the help of real-world examples Leverage Python 3 to develop malware and modify its complexities Book DescriptionPenetration testing enables you to evaluate the security or strength of a computer system, network, or web application that an attacker can exploit. With this book, you'll understand why Python is one of the fastest-growing programming languages for

penetration testing. You'll find out how to harness the power of Python and pentesting to enhance your system security. Developers working with Python will be able to put their knowledge and experience to work with this practical guide. Complete with step-by-step explanations of essential concepts and practical examples, this book takes a hands-on approach to help you build your own pentesting tools for testing the security level of systems and networks. You'll learn how to develop your own ethical hacking tools using Python and explore hacking techniques to exploit vulnerabilities in networks and systems. Finally, you'll be able to get remote access to target systems and networks using the tools you develop and modify as per your own requirements. By the end of this ethical hacking book, you'll have developed the skills needed for building cybersecurity tools and learned how to secure your systems by thinking like a hacker.What you will learn Understand the core concepts of ethical hacking Develop custom hacking tools from scratch to be used for ethical hacking purposes Discover ways to test the cybersecurity of an organization

by bypassing protection schemes Develop attack vectors used in real cybersecurity tests Test the system security of an organization or subject by identifying and exploiting its weaknesses Gain and maintain remote access to target systems Find ways to stay undetected on target systems and local networks Who this book is forIf you want to learn ethical hacking by developing your own tools instead of just using the prebuilt tools, this book is for you. A solid understanding of fundamental Python concepts is expected. Some complex Python concepts are explained in the book, but the goal is to teach ethical hacking, not Python. *Penetration Testing For Dummies* Adidas Wilson 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

The Basics of Hacking and Penetration Testing Packt Publishing Ltd You've done everything you can to logically secure your systems, along with layering in user education and providing physical security. However, the

only way to know if your defenses will hold is to test them. This course looks at one of the most important skills of any IT security professional: penetration testing. A key competency for the Certified Ethical Hacker exam, penetration testing is the process to check if a computer, system, network, or web application has any vulnerabilities. Cybersecurity expert Lisa Bock reviews the steps involved in performing a worthwhile penetration test, including auditing systems, listing and prioritizing vulnerabilities, and mapping out attack points a hacker might target. She also defines the various types of "pen" tests-such as black, grey, and white box; announced vs. unannounced; and automated vs. manual testing-and the techniques and blueprints a pen tester should use to test everything from Wi-Fi to VoIP. Finally, she discusses how to choose and work with an outsourced pen-testing organization, which can bring a valuable outsider's perspective to your IT security efforts.

The Basics of Hacking and Penetration Testing

Elsevier

This book explains the methodologies, framework, and "unwritten conventions"

that ethical hacks should employ to provide the maximum value to organizations that want to harden their security. It goes beyond the technical aspects of penetration testing to address the processes and rules of engagement for successful tests. The text examines testing from a strategic perspective to show how testing ramifications affect an entire organization. Security practitioners can use this book to reduce their exposure and deliver better service, while organizations will learn how to align the information about tools, techniques, and vulnerabilities that they gather from testing with their business objectives. Ethical Hacking: The Ultimate Guide to Using Penetration Testing to Audit and Improve the Cybersecurity of Computer Networks for Beginn John Wiley & Sons 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. *Penetration Testing Azure for Ethical Hackers* John Wiley & Sons This book gives you the skills you need to use Python for penetration testing, with the help of detailed code examples. This book has been updated for Python 3.6.3 and Kali Linux 2018.1. Key Features Detect and avoid various attack types that put the privacy of a system at risk Leverage Python to

build efficient code and eventually build a robust environment Learn about securing wireless applications and information gathering on a web server Book Description This book gives you the skills you need to use Python for penetration testing (pentesting), with the help of detailed code examples. We start by exploring the basics of networking with Python and then proceed to network hacking. Then, you will delve into exploring Python libraries to perform various types of pentesting and ethical hacking techniques. Next, we delve into hacking the application layer, where we start by gathering information from a website. We then move on to concepts related to website hacking—such as parameter tampering, DDoS, XSS, and SQL injection. By reading this book, you will learn different techniques and methodologies that will familiarize you with Python pentesting techniques, how to protect yourself, and how to create automated programs to find the admin console, SQL injection, and XSS attacks. What you will learn The basics of network pentesting including network scanning and sniffing Wireless,

wired attacks, and building traps for attack and torrent detection Web server footprinting and web application attacks, including the XSS and SQL injection attack Wireless frames and how to obtain information such as SSID, BSSID, and the channel number from a wireless frame using a Python script The importance of web server signatures, email gathering, and why knowing the server signature is the first step in hacking Who this book is for If you are a Python programmer, a security researcher, or an ethical hacker and are interested in penetration testing with the help of Python, then this book is for you. Even if you are new to the field of ethical hacking, this book can help you find the vulnerabilities in your system so that you are ready to tackle any kind of attack or intrusion.

Ethical Hacker's Certification Guide (CEHv11)

Newnes

This practical, tutorial-style book uses the Kali Linux distribution to teach Linux basics with a focus on how hackers would use them. Topics include Linux command line basics, filesystems, networking, BASH basics, package management, logging, and the Linux kernel and drivers. If you're getting started along

the exciting path of hacking, cybersecurity, and pentesting, Linux Basics for Hackers is an excellent first step. Using Kali Linux, an advanced penetration testing distribution of Linux, you'll learn the basics of using the Linux operating system and acquire the tools and techniques you'll need to take control of a Linux environment. First, you'll learn how to install Kali on a virtual machine and get an introduction to basic Linux concepts. Next, you'll tackle broader Linux topics like manipulating text, controlling file and directory permissions, and managing user environment variables. You'll then focus in on foundational hacking concepts like security and anonymity and learn scripting skills with bash and Python. Practical tutorials and exercises throughout will reinforce and test your skills as you learn how to: - Cover your tracks by changing your network information and manipulating the rsyslog logging utility - Write a tool to scan for network connections, and connect and listen to wireless networks - Keep your internet activity stealthy using Tor, proxy servers, VPNs, and encrypted email - Write a bash script to

scan open ports for potential targets - Use and abuse services like MySQL, Apache web server, and OpenSSH - Build your own hacking tools, such as a remote video spy camera and a password cracker Hacking is complex, and there is no single way in. Why not start at the beginning with Linux Basics for Hackers?

Hands on Hacking

Packt Publishing Ltd

The Basics of Hacking and Penetration Testing, Second Edition, serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. The book teaches students how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. It provides a simple and clean explanation of how to effectively utilize these tools, along with a four-step methodology for conducting a penetration test or hack, thus equipping students with the know-how required to jump start their careers and gain a better understanding of offensive security. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret

results and utilize those results in later phases. Tool coverage includes: Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. This is complemented by PowerPoint slides for use in class. This book is an ideal resource for security consultants, beginning InfoSec professionals, and students. Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Kali Linux distribution and focuses on the seminal tools required to complete a penetration test.

The Ethical Hack Packt Publishing Ltd 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 **Certified Ethical Hacker (CEH) Preparation Guide** Createspace Independent Publishing Platform Hacking (FREE Bonus Included)Lear n the Basics of Ethical Hacking and Penetration TestingIf you've ever read about computer hacking, you might be surprised to learn that companies actually pay people to try to hack into their systems. It's called "ethical hacking". Should you decide to learn to conduct ethical hacking, you will be responsible for helping organizations to protect their assets and information systems from malicious hackers, who would like to take advantage of any information

they can get their hands on. It's quite an interesting field of work, learning to legally hack into the systems of organizations like utility companies, banks and even government agencies. You will use the same skills as malicious hackers, but you will be using them for a much nobler purpose. Instead of trying to rip companies off, or steal secrets, you will be reporting the problems in their systems, so that they can repair them. Ethical hacking pays well, and it can easily be a full time job. Courses are available in various locations. You can research courses online and register for classes that will qualify you to be a certified ethical hacker. Here is what you will learn after reading this book: White hat hacking versus black hat and gray hat hacking How to hack into computer systems Reporting vulnerabilities to business management Becoming CEH certified as an ethical hacker Performing penetration testing Helping IT management to protect their sensitive information Getting Your FREE BonusRead this book, and find "BONUS: Your FREE Gift" chapter right after the introduction or after the conclusion. Python Ethical Hacking from Scratch IGI Global 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

Infrastructure Attack Strategies for Ethical Hacking Elsevier - Do you want learn how to build a PenTest Lab but you don't know where to start? - Do you want a practical book that explains step-by-step how to get going? - Do you want to become an Ethical Hacker or PenTester? If the answer is yes to the above questions, this book is for you! Frequently Asked Questions - Question: I am new to IT, and I don't have any experience in the field of Hacking, should I get this book? - Answer: This book is designed to those interested in Penetration Testing aka Ethical Hacking, and having limited, or no experience in the realm of Cybersecurity. -Question: I am not a hacker. Are there any technical prerequisites for reading this book? - Answer: No. This book is written in

everyday English, and no technical experience required. - Question: I have been reading similar books before, but I am still not sure if I should buy this book. How do I know this book is any good? - Answer: This book is written by a Security Architect, having over a decade of experience on platforms such as: Cisco Systems, Checkpoint, Palo Alto, Brocade, Back Track / Kali Linux, RedHat Linux, CentOS, Orion, Prime, DLP, IPS, IDS, Nexus, and much more... Learning from someone with real life experience is extremely valuable. You will learn about real life technologies and methodologies used in today's IT Infrastructure, and Cybersecurity Division. BUY THIS BOOK NOW, AND GET STARTED TODAY! IN THIS BOOK YOU WILL LEARN: What are the Foundations of Penetration Testing What are the Benefits of Penetration Testing What are the Frameworks of Penetration Testing What Scanning Tools you should be Aware What Credential Testing Tools you must Utilize What Debugging & Software Assurance Tools are Available Introduction to OSINT & Wireless Tools What is a Web Proxy, SET & RDP What Mobile Tools you should be familiar with How Communicatio

n must take place How to Cover your Back How to Setup a Lab in NPE How to Setup Hyper-V on Windows 10 How to Setup VMware on Windows 10 How to Assemble the Required Resources How to Install Windows Server in VMware How to Configure Windows Server in VMware How to Install Windows Server in Hyper-V How to Configure Windows Server in Hyper-V How to Install & Configure OWASP-BWA in VMware How to Install & Configure Metasploitable in VMware How to Install Kali Linux in VMware How to Install BlackArch in Hyper-V What Categories of Penetration Tests exists What Software & Hardware you must have as a PenTester Understanding Confidentiality What are the Rules of Engagement How to set Objectives & Deliverables What Type of Targets you must deal with Specialized Systems for Pen Testers How to Identify & Response to Risk How to Prepare your Pen Test Team for an Engagement What are the Best Practices before Going Live BUY THIS BOOK NOW, AND GET STARTED TODAY!

Kali Linux - An Ethical Hacker's Cookbook

Independently Published

Discover end-to-end penetration testing solutions to enhance your ethical hacking skills

Key FeaturesPractical recipes to conduct effective penetration testing using the latest version of Kali LinuxLeverage tools like Metasploit, Wireshark, Nmap, and more to detect vulnerabilities with easeConfidently perform networking and application attacks using task-oriented recipesBook Description Many organizations have been affected by recent cyber events. At the current rate of hacking, it has become more important than ever to pentest your environment in order to ensure advanced-level security. This book is packed with practical recipes that will quickly get you started with Kali Linux (version 2018.4 / 2019), in addition to covering the core functionalities. The book will get you off to a strong start by introducing you to the installation and configuration of Kali Linux, which will help you to perform your tests. You will also learn how to plan attack strategies and perform web application exploitation using tools such as Burp and JexBoss. As you progress, you will get to grips with performing network exploitation using Metasploit, Sparta, and Wireshark. The book will also help you delve into the technique of

carrying out wireless and password attacks using tools such as Patator, John the Ripper, and airoscript-ng. Later chapters will draw focus to the wide range of tools that help in forensics investigations and incident response mechanisms. As you wrap up the concluding chapters, you will learn to create an optimum quality pentest report. By the end of this book, you will be equipped with the knowledge you need to conduct advanced penetration testing, thanks to the book's crisp and task-oriented recipes. What you will learnLearn how to install, set up and customize Kali for pentesting on multiple platformsPentest routers and embedded devicesGet insights into fiddling around with software-defined radioPwn and escalate through a corporate networkWrite good quality security reportsExplore digital forensics and memory analysis with Kali LinuxWho this book is for If you are an IT security professional, pentester, or security analyst who wants to conduct advanced penetration testing techniques, then this book is for you. Basic knowledge of Kali Linux is assumed.

The Pentester BluePrint

Packt

Publishing Ltd You will learn how to properly utilize and interpret the results of modern day hacking tools, which are required to complete a penetration test. Tool coverage includes Backtrack and Kali Linux, Google reconnaissance, MetaGooFil, DNS interrogation, Nmap, Nessus, Metasploit, the Social Engineer Toolkit (SET), w3af, Netcat, post exploitation tactics, the Hacker Defender rootkit, and more. The book provides a simple and clean explanation of how to effectively utilize the tools and introduces a four-step methodology for conducting a penetration test or hack. You will be provided with the know-how required to jump start your career or gain a better understanding of offensive security. The book walks through each of the steps and tools in a structured, orderly manner, allowing readers to understand how the output from each tool can be fully utilized in the subsequent phases of the penetration test. This process allows readers to clearly see how the tools and phases function and relate.-The second edition includes updated information covering Kali Linux as well as focusing on the seminal tools required

to complete a penetration testNew tools added including the Social Engineer Toolkit, Meterpreter, w3af and more!Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases

The New Penetrating Testing for Beginners BPB Publications

The Basics of Hacking and Penetration Testing serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. This book makes ethical hacking and penetration testing easy – no prior hacking experience is required. It shows how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. With a simple and clean explanation of how to effectively utilize these tools – as well as the introduction to a four-step methodology for conducting a penetration test or hack – the book provides students with the know-how required to jump start their careers and gain a better understanding of offensive security. The book is organized into 7 chapters that cover hacking tools such as

Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. PowerPoint slides are available for use in class. This book is an ideal reference for security consultants, beginning InfoSec professionals, and students. Named a 2011 Best Hacking and Pen Testing Book by InfoSec Reviews Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Writen by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Backtrack Linus distribution and focuses on the seminal tools required to complete a penetration test. Learning Kali Linux Orange Education Pvt Ltd Penetration testers simulate cyber attacks to find security weaknesses in networks,

operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–base d lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—i ncluding information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own Metasploit modules –Automate social-engineering attacks –Bypass antivirus software –Turn access to one machine into total control of the enterprise

in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.

Web Penetration Testing with Kali Linux

Apress

You will learn how to properly utilize and interpret the results of modern day hacking tools, which are required to complete a penetration test. Tool coverage includes Backtrack and Kali Linux, Google reconnaissance, MetaGooFil, DNS interrogation, Nmap, Nessus, Metasploit, the Social Engineer Toolkit (SET), w3af, Netcat, post exploitation tactics, the Hacker Defender rootkit, and more. The book provides a simple and clean explanation of how to effectively utilize the tools and introduces a four-step methodology for conducting a penetration test or hack. You will be provided with the know-how required to jump start your career or gain a better understanding of offensive security. The book walks

through each of the steps and tools in a structured, orderly manner, allowing readers to understand how the output from each tool can be fully utilized in the subsequent phases of the penetration test. This process allows readers to clearly see how the tools and phases function and relate.-The second edition includes updated information covering Kali Linux as well as focusing on the seminal tools required to complete a penetration test New tools added including the Social Engineer Toolkit, Meterpreter, w3af and more!Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases *Ethical Hacking and Penetration Testing Guide* John Wiley & Sons Know the basic principles of ethical hacking. This book is designed to provide you with the knowledge, tactics, and tools needed to prepare for the Certified Ethical Hacker(CEH) exam—a qualification that tests the cybersecurity professional's baseline knowledge of security threats, risks, and countermeasures through lectures and hands-on labs. You will review the

organized certified hacking mechanism along with: stealthy network re-con; passive traffic detection; privilege escalation, vulnerability recognition, remote access, spoofing; impersonation, brute force threats, and cross-site scripting. The book covers policies for penetration testing and requirements for documentation. This book uses a unique “lesson” format with objectives and instruction to succinctly review each major topic, including: footprinting and reconnaissance and scanning networks, system hacking, sniffers and social engineering, session hijacking, Trojans and backdoor viruses and worms, hacking webservers, SQL injection, buffer overflow, evading IDS, firewalls, and honeypots, and much more. What You Will learn Understand the concepts associated with Footprinting Perform active and passive reconnaissance Identify enumeration countermeasures Be familiar with virus types, virus detection methods, and virus countermeasures Know the proper order of steps used to conduct a session hijacking attack Identify defensive strategies against SQL injection

attacks Analyze internal and external network traffic using an intrusion detection system Who This Book Is For Security professionals looking to get this credential, including systems administrators, network administrators, security administrators, junior IT auditors/penetration testers, security specialists, security consultants, security engineers, and more