Learning Kali Linux Security Testing Penetration

As recognized, adventure as with ease as experience not quite lesson, amusement, as capably as concord can be gotten by just checking out a book **Learning Kali Linux Security Testing Penetration** along with it is not directly done, you could put up with even more around this life, going on for the world.

We manage to pay for you this proper as without difficulty as simple habit to acquire those all. We meet the expense of Learning Kali Linux Security Testing Penetration and numerous book collections from fictions to scientific research in any way. in the midst of them is this Learning Kali Linux Security Testing Penetration that can be your partner.

Penetration Testing mit mimikatz - Sebastian Brabetz 2020-11-18
• Penetration Tests mit mimikatz von Pass-the-Hash über Kerberoasting bis hin zu Golden Tickets • Funktionsweise und Schwachstellen der Windows Local Security Authority (LSA) und des Kerberos-Protokolls • Alle Angriffe leicht verständlich und Schritt für Schritt erklärt mimikatz ist ein extrem leistungsstarkes Tool für Angriffe auf das Active Directory. Hacker können damit auf Klartextpasswörter, Passwort-Hashes sowie Kerberos Tickets zugreifen, die dadurch erworbenen Rechte in fremden Systemen ausweiten und so die Kontrolle über ganze Firmennetzwerke übernehmen. Aus diesem Grund ist es wichtig, auf Angriffe mit mimikatz vorbereitet zu sein. Damit Sie die Techniken der Angreifer verstehen und erkennen können, zeigt Ihnen IT-Security-Spezialist Sebastian Brabetz in diesem Buch, wie Sie Penetration Tests mit mimikatz in einer sicheren Testumgebung durchführen. Der Autor beschreibt alle Angriffe Schritt für Schritt und erläutert ihre Funktionsweisen leicht verständlich. Dabei setzt er nur grundlegende IT-Security-Kenntnisse voraus. Sie lernen insbesondere folgende Angriffe kennen: - Klartextpasswörter aus dem RAM extrahieren - Authentifizierung ohne Klartextpasswort mittels - Pass-the-Hash - Ausnutzen von Kerberos mittels Overpass-the-Hash, Pass-the-Key und Pass-the-Ticket - Dumpen von Active Directory Credentials aus Domänencontrollern - Erstellen von Silver Tickets und Golden Tickets - Cracken der Passwort-Hashes von Service Accounts mittels Kerberoasting - Auslesen und Cracken von Domain Cached Credentials Darüber hinaus erfahren Sie, wie Sie die Ausführung von mimikatz sowie die Spuren von mimikatz-Angriffen erkennen. So sind Sie bestens gerüstet, um Ihre Windows-Domäne mit mimikatz auf Schwachstellen zu testen und entsprechenden Angriffen vorzubeugen.
Hands-On Penetration Testing with Kali NetHunter - Glen D. Singh 2019-02-28
Convert Android to a powerful pentesting platform. Key FeaturesGet up and running with Kali Linux NetHunter Connect your Android device and gain full control over Windows, OSX, or Linux devices Crack Wi-Fi passwords and gain access to devices connected over the same network collecting intellectual dataBook Description Kali NetHunter is a version of the popular and powerful Kali Linux pentesting platform, designed to be installed on mobile devices. Hands-On Penetration Testing with Kali NetHunter will teach you the components of NetHunter and how to install the software. You'll also learn about the different tools included and how to optimize and use a package, obtain desired results, perform tests, and make your environment more secure. Starting with an introduction to Kali NetHunter, you will delve into different phases of the pentesting process. This book will show you how to build your penetration testing environment and set up your lab. You will gain insight into gathering intellectual data, exploiting vulnerable areas, and gaining control over target systems. As you progress through the book, you will explore the NetHunter tools available for exploiting wired and wireless devices. You will work through new ways to deploy existing tools designed to reduce the chances of detection. In the concluding chapters, you will discover tips and best practices for integrating security hardening into your Android ecosystem. By the end of this book, you will have learned to successfully use a mobile penetration testing device based on Kali NetHunter and Android to accomplish the same tasks you would traditionally, but in a smaller and more mobile form factor. What you will learnChoose and configure a hardware device to use Kali NetHunter Use various tools during pentests Understand NetHunter suite components Discover tips to effectively use a compact mobile platform Create your own Kali NetHunter-enabled device and configure it for optimal results Learn to scan and gather information from a target Explore hardware adapters for testing and auditing wireless networks and Bluetooth devicesWho this book is for Hands-On Penetration Testing with Kali NetHunter is for pentesters, ethical hackers, and security professionals who want to learn to use Kali NetHunter for complete mobile penetration testing and are interested in venturing into the mobile domain. Some prior understanding of networking assessment and Kali Linux will be helpful.
Kali Linux Network Scanning Cookbook - Michael Hixon 2017-05-26
Over 100 practical recipes that leverage custom scripts and integrated tools in Kali Linux to help you effectively master network scanningAbout This Book* Learn the fundamentals behind commonly used scanning techniques* Deploy powerful scanning tools that are integrated into the Kali Linux testing platform* The practical recipes will help you automate menial tasks and build your own script libraryWho This Book Is ForThis book is for information security professionals and casual security enthusiasts alike. It provides foundational principles if you"re a novice, but will also introduce scripting techniques and in-depth analysis if you"re more advanced. Whether you are brand new to Kali Linux or a seasoned veteran, this book will help you both understand and ultimately master many of the most powerful and useful scanning techniques in the industry. It is assumed that you have some basic security testing experience.What You Will Learn* Develop a network-testing environment to test scanning tools and techniques* Understand the principles of network-scanning tools by building scripts and tools* Identify distinct vulnerabilities in web apps and remote services and learn how they are exploited* Perform comprehensive scans to identify listening on TCP and UDP sockets* Get started with different Kali desktop environments--KDE, MATE, LXDE, and Xfce* Use Sparta for information gathering, port scanning, fingerprinting, vulnerability scanning, and more* Evaluate DoS threats and learn how common DoS attacks are performed* Learn how to use Burp Suite to evaluate web applicationsIn DetailWith the ever-increasing amount of data flowing in today"s world, information security has become vital to any application. This is where Kali Linux comes in. Kali Linux focuses mainly on security auditing and penetration testing. This step-by-step cookbook on network scanning trains you in important scanning concepts based on version 2016.2. It will enable you to conquer any network environment through a range of network scanning techniques and will also equip you to script your very own tools.Starting with the fundamentals of installing and managing Kali Linux, this book will help you map your target with a wide range of network scanning tasks, including discovery, port scanning, fingerprinting, and more. You will learn how to utilize the arsenal of tools available in Kali Linux to conquer any network environment. The book offers expanded coverage of the popular Burp Suite and has new and updated scripts for automating scanning and target exploitation. You will also be shown how to identify remote services, how to assess security risks, and how various attacks are performed. You will cover the latest features of Kali Linux 2016.2, which includes the enhanced Sparta tool and many other exciting updates.This immersive guide will also encourage the creation of personally scripted tools and the skills required to create them.Style and approachThis step-by-step guide is full of recipes that will help you use integrated scanning tools in Kali Linux and develop custom scripts to make new and unique tools of your own.
Kali Linux - Anastasia Sharp 2022-01-21
You are about to discover how to start hacking with the #1 hacking/penetration testing tool, Kali Linux, in no time, even if you've never hacked before! Kali Linux is the king of all penetration testing tools out there. But while its 600+ pre-installed tools and utilities are meant to make penetration testing and forensics easy, at first, it can be overwhelming for experienced and aspiring security professionals to decide which tool to use to conduct a specific penetration test. That's where this book comes in to streamline your learning experience! If you are uncertain about where to begin even after reading and watching tons of free information online, this book will give you the much needed structure to go all in into the world of ethical hacking into secure computer systems with the best tool for the job. Since its introduction in

2012 as a successor to the previous version, Back Track Linux, Kali Linux has grown in popularity and capabilities to become the go-to open source security tool for information security professionals around the world. And this book will show you how to use it like the pros use it even if you've never stepped into a formal Kali Linux class before! In this book, we are going to cover the major features & tools provided by Kali Linux, including: Downloading, installation and set up Information gathering tools Vulnerability assessment Wireless attacks Web application attacks Exploitation tools Forensics tools Sniffing and spoofing Password cracking Maintaining access Social engineering tools Reverse engineering tools Hardware hacking tools Reporting tools Denial of service attacks And much more! We shall cover each of these features & tools individually so that after reading this guide, you have hands-on experience with using Kali Linux and can use what you learn when completing the hands-on Kali Linux practice project found in the part 17 of this guide. To make the learning experience faster and easier for you, for this hands-on, Kali Linux guide, we may have to install some other tools needed to make it easier to learn how to use Kali Linux for penetration testing and cyber security forensics. Everything is laid out with easy to follow examples and illustrations to help you to follow through, practice and ultimately remember whatever you are learning!

Mastering Kali Linux for Advanced Penetration Testing - Second Edition - Vijay Kumar Velu 2017-06-30

A practical guide to testing your network's security with Kali Linux, the preferred choice of penetration testers and hackers.About This Book* Employ advanced pentesting techniques with Kali Linux to build highly-secured systems* Get to grips with various stealth techniques to remain undetected and defeat the latest defenses and follow proven approaches* Select and configure the most effective tools from Kali Linux to test network security and prepare your business against malicious threats and save costsWho This Book Is ForPenetration Testers, IT professional or a security consultant who wants to maximize the success of your network testing using some of the advanced features of Kali Linux, then this book is for you.Some prior exposure to basics of penetration testing/ethical hacking would be helpful in making the most out of this title. What You Will Learn* Select and configure the most effective tools from Kali Linux to test network security* Employ stealth to avoid detection in the network being tested* Recognize when stealth attacks are being used against your network* Exploit networks and data systems using wired and wireless networks as well as web services* Identify and download valuable data from target systems* Maintain access to compromised systems* Use social engineering to compromise the weakest part of the network--the end usersIn DetailThis book will take you, as a tester or security practitioner through the journey of reconnaissance, vulnerability assessment, exploitation, and post-exploitation activities used by penetration testers and hackers.We will start off by using a laboratory environment to validate tools and techniques, and using an application that supports a collaborative approach to penetration testing. Further we will get acquainted with passive reconnaissance with open source intelligence and active reconnaissance of the external and internal networks. We will also focus on how to select, use, customize, and interpret the results from a variety of different vulnerability scanners. Specific routes to the target will also be examined, including bypassing physical security and exfiltration of data using different techniques. You will also get to grips with concepts such as social engineering, attacking wireless networks, exploitation of web applications and remote access connections. Later you will learn the practical aspects of attacking user client systems by backdooring executable files. You will focus on the most vulnerable part of the network--directly and bypassing the controls, attacking the end user and maintaining persistence access through social media.You will also explore approaches to carrying out advanced penetration testing in tightly secured environments, and the book's hands-on approach will help you understand everything you need to know during a Red teaming exercise or penetration testingStyle and approachAn advanced level tutorial that follows a practical approach and proven methods to maintain top notch security of your networks.

Web Penetration Testing with Kali Linux - Third Edition - Gilberto Najera-Gutierrez 2018-02-28

Build your defense against web attacks with Kali Linux, including command injection flaws, crypto implementation layers, and web application security holes Key Features Know how to set up your lab with Kali Linux Discover the core concepts of web penetration testing Get the tools and techniques you need with Kali Linux Book Description Web Penetration Testing with Kali Linux - Third Edition shows you how to set up a lab, helps you understand the nature and mechanics of attacking websites, and explains classical attacks in great depth. This edition is heavily updated for the latest Kali Linux changes and the most recent attacks. Kali Linux shines when it comes to client-side attacks and fuzzing in particular. From the start of the book, you'll be given a thorough grounding in the concepts of hacking and penetration testing, and you'll see the tools used in Kali Linux that relate to web application hacking. You'll gain a deep understanding of classicalSQL, command-injection flaws, and the many ways to exploit these flaws. Web penetration testing also needs a general overview of client-side attacks, which is rounded out by a long discussion of scripting and input validation flaws. There is also an important chapter on cryptographic implementation flaws, where we discuss the most recent problems with cryptographic layers in the networking stack. The importance of these attacks cannot be overstated, and defending against them is relevant to most internet users and, of course, penetration testers. At the end of the book, you'll use an automated technique called fuzzing to identify flaws in a web application. Finally, you'll gain an understanding of web application vulnerabilities and the ways they can be exploited using the tools in Kali Linux. What you will learn Learn how to set up your lab with Kali Linux Understand the core concepts of web penetration testing Get to know the tools and techniques you need to use with Kali Linux Identify the difference between hacking a web application and network hacking Expose vulnerabilities present in web servers and their applications using server-side attacks Understand the different techniques used to identify the flavor of web applications See standard attacks such as exploiting cross-site request forgery and cross-site scripting flaws Get an overview of the art of client-side attacks Explore automated attacks such as fuzzing web applications Who this book is for Since this book sets out to cover a large number of tools and security fields, it can work as an introduction to practical security skills for beginners in security. In addition, web programmers and also system administrators would benefit from this rigorous introduction to web penetration testing. Basic system administration skills are necessary, and the ability to read code is a must.

Hacken mit Kali-Linux - Mark B. 2020-08-03

Bei meiner Arbeit stoße ich immer wieder auf Netzwerke und Webseiten mit erheblichen Sicherheitsproblemen. In diesem Buch versuche ich dem Leser zu vermitteln, wie leicht es mittlerweile ist, Sicherheitslücken mit diversen Tools auszunutzen. Daher sollte meiner Meinung nach jeder, der ein Netzwerk oder eine Webseite betreibt, ansatzweise wissen, wie diverse Hackertools arbeiten, um zu verstehen, wie man sich dagegen schützen kann. Selbst vor kleinen Heimnetzwerken machen viele Hacker nicht halt. Wenngleich das Thema ein sehr technisches ist, werde ich dennoch versuchen, die Konzepte so allgemein verständlich wie möglich erklären. Ein Informatikstudium ist also keinesfalls notwendig, um diesem Buch zu folgen. Dennoch will ich nicht nur die Bedienung diverser Tools erklären, sondern auch deren Funktionsweise so weit erklären, dass Ihnen klar wird, wie das Tool arbeitet und warum ein bestimmter Angriff funktioniert.

Basic Security Testing with Kali Linux, Third Edition - Daniel W. Dieterle 2018-08-22

Basic Security Testing with Kali Linux, Third Edition Kali Linux (2018) is an Ethical Hacking platform that allows security professionals to use the same tools and techniques that a hacker would use, so they can find security issues before the attackers do. In Basic Security Testing with Kali Linux, you will learn basic examples of how hackers find out information about your company, find weaknesses in your security, how they gain access to your systems, and most importantly, how to stop them. Completely updated for 2018, this hands on step-by-step guide covers: Kali Linux Overview & Usage Shodan (the "Hacker's Google") Metasploit Tutorials Exploiting Windows and Linux Systems Escalating Privileges in Windows Cracking Passwords and Obtaining Clear Text Passwords Wi-Fi Attacks Kali on a Raspberry Pi & Android Securing your Network And Much More! /ul> Though no computer can be completely "Hacker Proof" knowing how an attacker works will help put you on the right track of better securing your network!

Python 3 - Johannes Ernesti 2017

Learning Kali Linux - Ric Messier 2018-07-17

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

Mastering Kali Linux for Advanced Penetration Testing - Vijay Kumar Velu 2017-06-30

A practical guide to testing your network's security with Kali Linux, the preferred choice of penetration testers and hackers. About This Book Employ advanced pentesting techniques with Kali Linux to build highly-secured systems Get to grips with various stealth techniques to remain undetected and defeat the latest defenses and follow proven approaches Select and configure the most effective tools from Kali Linux to test network security and prepare your business against malicious threats and save costs Who This Book Is For Penetration Testers, IT professional or a security consultant who wants to maximize the success of your network testing using some of the advanced features of Kali Linux, then this book is for you.Some prior exposure to basics of penetration testing/ethical hacking would be helpful in making the most out of this title. What You Will Learn Select and configure the most effective tools from Kali Linux to test network security Employ stealth to avoid detection in the network being tested Recognize when stealth attacks are being used against your network Exploit networks and data systems using wired and wireless networks as well as web services Identify and download valuable data from target systems Maintain access to compromised systems Use social engineering to compromise the weakest part of the network—the end users In Detail This book will take you, as a tester or security practitioner through the journey of reconnaissance, vulnerability assessment, exploitation, and post-exploitation activities used by penetration testers and hackers. We will start off by using a laboratory environment to validate tools and techniques, and using an application that supports a collaborative approach to penetration testing. Further we will get acquainted with passive reconnaissance with open source intelligence and active reconnaissance of the external and internal networks. We will also focus on how to select, use, customize, and interpret the results from a variety of different vulnerability scanners. Specific routes to the target will also be examined, including bypassing physical security and exfiltration of data using different techniques. You will also get to grips with concepts such as social engineering, attacking wireless networks, exploitation of web applications and remote access connections. Later you will learn the practical aspects of attacking user client systems by backdooring executable files. You will focus on the most vulnerable part of the network—directly and bypassing the controls, attacking the end user and maintaining persistence access through social media. You will also explore approaches to carrying out advanced penetration testing in tightly secured environments, and the book's hands-on approach will help you understand everything you need to know during a Red teaming exercise or penetration testing Style and approach An advanced level tutorial that follows a practical approach and proven methods to maintain top notch security of your networks.

Mehr Hacking mit Python - Justin Seitz 2015-10-09

Wenn es um die Entwicklung leistungsfähiger und effizienter Hacking-Tools geht, ist Python für die meisten Sicherheitsanalytiker die Sprache der Wahl. Doch wie genau funktioniert das? In dem neuesten Buch von Justin Seitz - dem Autor des Bestsellers "Hacking mit Python" - entdecken Sie Pythons dunkle Seite. Sie entwickeln Netzwerk-Sniffer, manipulieren Pakete, infizieren virtuelle Maschinen, schaffen unsichtbare Trojaner und vieles mehr. Sie lernen praktisch, wie man • einen "Command-and-Control"-Trojaner mittels GitHub schafft • Sandboxing erkennt und gängige Malware-Aufgaben wie Keylogging und Screenshotting automatisiert • Windows-Rechte mittels kreativer Prozesskontrolle ausweitet • offensive Speicherforensik-Tricks nutzt, um Passwort-Hashes abzugreifen und Shellcode in virtuelle Maschinen einzuspeisen • das beliebte Web-Hacking-Tool Burp erweitert • die Windows COM-Automatisierung nutzt, um einen Man-in-the-Middle-Angriff durchzuführen • möglichst unbemerkt Daten aus einem Netzwerk abgreift Eine Reihe von Insider-Techniken und kreativen Aufgaben zeigen Ihnen, wie Sie die Hacks erweitern und eigene Exploits entwickeln können.

HACKING WITH KALI LINUX - Larry T. Deering 2021-02-22

Kali Linux is developed, funded and maintained by a leading company called Offensive Security. It's a Penetration Testing and Password Cracker distribution, used for Ethical Hacking and for network security assesments. Hacking with Kali Linux is the guide to effectively hacking from zero to one hundred percent.In this book you will learn directly how everything works, what processes and programs should be used and how you can become successful hackers with Kali Linux. Being a Ethical can help you to build strong defences against piracy and protect your data and networks. Here's something you will learn: - Improving Your Cyber Security - Learning Cyber Security Foundations - How To Defend Your Computer Against Hackers - Kali Tools - How To Hack A Wireless Network Each chapter of this fantastic book is full of technical language that you will learn step-by-step. With "Hacking with Kali Linux" you will become an ethical hacker sooner as you imagine. So, what are you waiting? Buy now and enjoy! Learn CyberSecurity. Improve And Master Security Testing, Penetration Testing, and Ethical Hacking

Kali Linux - Raymond Deep 2020-11-18

If you want to learn about Kali Linux but aren't sure where to start then keep reading... Does the world of cybersecurity seem exciting, but a little overwhelming to grasp?Do you want to learn about ethical hacking?IF YES, then this is the perfect book for you. Our dependence on technology is increasing by the day. Gone are the days when a crime was restricted to the physical realm alone! These days, crime has seeped into the virtual world too! Cybercrimes have become rampant, and with it, the need for cybersecurity is ever increasing. A single attack on an organization's network can cause irreparable harm to the company's assets as well as reputation. Learning about cybersecurity, along with ethical hacking using Kali Linux gives you all the practical information you require for developing your skills as a professional in the industry of information security. Apart from this, it also provides you with plenty of excitement as well as exhilaration which are associated with the world of computers and network hacking. Kali Linux is the successor of the BackTrack Linux operating system. BackTrack Linux was developed for the same tasks, which mainly aimed at penetration testing and digital forensics. BackTrack Linux was deprecated in 2013 and rebooted completely with a new name Kali. Kali complies with all the Debian development standards from top to bottom. Kali Linux is an open-source model, has over 600 types of tools, provides multi-language support, is fully customizable, and it doesn't cost a penny to use. These are some of the most notable benefits associated with using Kali Linux. Kali Linux is considered to be among the best open-source security packages available for an ethical hacker. It contains a base set of tools which are divided into different categories. This can be easily installed on a machine in the form of an operating system and is a practical option because it has a wider scope for working and combining various tools. This book is the perfect guide for all beginners who want to understand the fundamentals of Kali Linux. Apart from them, it is also well-suited for all those who are professionally engaged in the field of penetration testing. This book is geared at beginners, but if you are already familiar with certain basic concepts associated with any Linux operating system, learning about Kali Linux, ethical hacking, and cybersecurity will become easier. In this book, you will learn about All the features of Kali LinuxSteps to download and install Kali LinuxKali Linux commandsHacking, ethical hacking, and cybersecurityKali Linux Tools, and much more! Even if it is your first approach with hacking, by the end of this book you will be armed with all the knowledge you require to get started in ethical hacking. Even if you are a complete beginner, this book will act as your guide as you traverse the virtual world. So, what are you waiting for? If you are eager to step into the world of ethical hacking and cybersecurity, then SCROLL UP THE PAGE AND GRAB YOUR COPY TODAY CLICKING "BUY NOW" button!

Kali Linux Web Penetration Testing Cookbook - Gilberto Najera Gutierrez 2018-08-31

Discover the most common web vulnerabilities and prevent them from becoming a threat to your site's security Key Features Familiarize yourself with the most common web vulnerabilities Conduct a preliminary assessment of attack surfaces and run exploits in your lab Explore new tools in the Kali Linux ecosystem for web penetration testing Book Description Web applications are a huge point of attack for malicious hackers and a critical area for security professionals and

penetration testers to lock down and secure. Kali Linux is a Linux-based penetration testing platform that provides a broad array of testing tools, many of which can be used to execute web penetration testing. Kali Linux Web Penetration Testing Cookbook gives you the skills you need to cover every stage of a penetration test - from gathering information about the system and application, to identifying vulnerabilities through manual testing. You will also cover the use of vulnerability scanners and look at basic and advanced exploitation techniques that may lead to a full system compromise. You will start by setting up a testing laboratory, exploring the latest features of tools included in Kali Linux and performing a wide range of tasks with OWASP ZAP, Burp Suite and other web proxies and security testing tools. As you make your way through the book, you will learn how to use automated scanners to find security flaws in web applications and understand how to bypass basic security controls. In the concluding chapters, you will look at what you have learned in the context of the Open Web Application Security Project (OWASP) and the top 10 web application vulnerabilities you are most likely to encounter, equipping you with the ability to combat them effectively. By the end of this book, you will have acquired the skills you need to identify, exploit, and prevent web application vulnerabilities. What you will learn Set up a secure penetration testing laboratory Use proxies, crawlers, and spiders to investigate an entire website Identify cross-site scripting and client-side vulnerabilities Exploit vulnerabilities that allow the insertion of code into web applications Exploit vulnerabilities that require complex setups Improve testing efficiency using automated vulnerability scanners Learn how to circumvent security controls put in place to prevent attacks Who this book is for Kali Linux Web Penetration Testing Cookbook is for IT professionals, web developers, security enthusiasts, and security professionals who want an accessible reference on how to find, exploit, and prevent security vulnerabilities in web applications. The basics of operating a Linux environment and prior exposure to security technologies and tools are necessary.

Hacking with Kali Linux - Mark Coding 2020-11-27

Are you interested in finding new and effective ways to keep your system safe and secure?Do you want to make sure you are not going to be attacked online, and that you won't have to worry about your personal or financial information getting into the wrong hands? Are you worried about some of the attacks and the headlines going around right now concerning data breaches and hackers, and you want to make sure you stay safe and secure? The Kali Linux operating system is one of the best options to work with when you are ready to try out some hacking in an ethical and safe manner. Using some of the same techniques that many hackers are going to rely on, you can learn some of the different methods they are going to use, and figure out where your potential vulnerabilities are right from the start. When you know where these vulnerabilities are, it is so much easier to fix them and keep your network as safe as possible. Inside this guidebook, we are going to spend some time taking a look at the Kali Linux system and how we are able to use it to help with protecting our systems. From learning how to work with a VPN to completing our own penetration test and network scan, this system is going to help keep you as safe and secure as possible. Some of the different topics we will explore to help out with this goal include: -History of Kali Linux and some of the benefits of working with this operating system. -Some of the basics and the commands you need to use in order to get started with this language. -How to download and install the Kali Linux operating system. -The importance of working on your cybersecurity and keeping your system safe. -How to handle your own penetration testing to make sure your computer system is safe and to figure out where we can fix some vulnerabilities -The different types of hackers we need to be aware of and how they all work differently from one another. -The different types of attacks that can happen when we are going to work with a hacker and that we need to be prepared for. -Some of the steps you are able to take in order to keep your system safe and secure from others. Protecting your system and your computer safe from hackers can be important in ensuring your personal information is going to stay as safe and secure as possible. When you are ready to learn how to use the Kali Linux operating system, to make this happen, make sure to check out this guidebook to help you get started.

Kali Linux For Beginners - Learn Computer Hacking In Deep 2020-10-18

If You Are Very Much Worried About The Security Structure Of Your Network Or Server And Want To Prevent All Forms Of Attacks Along With Vulnerabilities On Your System, Then Keep Reading You might come across several problems at the time of installing Kali Linux on your system (and it is not funny). Also, if you are unable to install the same properly, you will fail in getting access this awesome softwere and you will be irritated. But just like existing problems, there is also a wide range of troubleshooters which yuo can learn through this book helping in getting rid of all forms of problems that come in the way of installation. But why is kali linux so improrantantant to have? You need to know that Kali Linux is much more than just hacking. It comes with some advanced forms of features which can help in making your tasks of programming along with hacking lot more easier. But this software does not only provide help at the time of hacking but it also comes along with various tools which helps the users in testing out their networks for finding out the vulnerabilities in their network or system. I know programming and hacking in Linux can be tough but thanks to this excellent book you will receive the proper knowledge about the functioning of Kali Linux regarding programming and hacking, thus you will be able to program and hack without any form of problem in this software. Furthermore Kali Linux is integrated with several functions which when carried out together, can actually do wonders. It can be regarded among the most effective software in today's world. Most of the big companies today seek the help of Kali Linux for the purpose of tracing and checking the various forms of vulnerabilities which are present within a system and thus ensures 100% security for an organization. Unless and until you are unaware of the basics, you will not be able to use this software. In fact for carrying out an effective form of ethical hacking, you will need to learn about the various attacks along with the forms of networks. You can easily find this information in this book. Here is some of all the main elements which you can find in this book: -Installing and Downloading Kali LinuxTroubleshooting installations-Essential and advanced Linux terminal command-Adding and removing software -Controlling file and directory permissions-Real world application for kali Linux and useful tools-Programming in Linux using: C, C++, Python, Java, Bash-Network Basics-Wireless hacking and penetration testing with Linux -How to carry out an effective attackAnd Much More! Okay, but why can this book help me? Because this book will give you a detailed structure about the installation of Kali Linux software on your system and how you can configure the same. The chapters that you are going to find in this book are arranged with information, exercises and explanations in a very orderly manner which can easily answer all your questions and can clear all your doubts regarding hacking and Kali Linux. This book will be the perfect choice for you. It is something which you really need to have if you want to improve the security of your system or if you want to learn programming by using Kali Linux. Even if you have never installed kali linux in your computer; Even if you do not know anything about programming and hacking, do not worry because this book has been designed for peaple like you! Click on "Buy Now " and Get Your Copy Now!

Hacking for Beginners - T. Y. E. DARWIN 2020-09-23

5 topics of Hacking you need to learn right now□□□□□ What is Hacking?♥ Hacking is a Skill. Hacking is a practice. Hacking is a passion. To be a hacker you need not build things but you need to crack them. Hackers are always decipted as evil in popular cultural references. However, there are good hackers called as " Ethical hackers " also known as " Penetration testers" and "security researchers". This book is written by a penetration researcher who have 20 years experience in the industry. He had spent time with hundreds of hackers and security researchers and compiled all his thoughts into this book. Hacking is not easy. But if you can follow a pathway followed by thousands of hackers from years ago you can easily become one. Author of this book explains these hacking procedures in 5 parts for your easy understanding. The five parts that are discussed in this paperback are :□□□□□ Creating a Perfect Hacking Environment Information Gathering Scanning and Sniffing (To Automatically find Vulnerabilities) Metasploit (To develop exploits and Bind them) Password Cracking (To crack passwords of Wifi and Websites) Why to buy this book? Are you a programmer trying to build things and unaware of the problems that may arise if you don't use good security practices in your code? Then you need to use this guide to create code that can not be able to be cracked by hackers. Are you a beginner who is interested in Hacking but are unaware of the roadmap that need to be used to become an elite hacker? Then you should read this to get a complete understanding about hacking principles Are you a bug-bounty hunter trying to build exploits to earn money? Then you should use this to expand your core hacking knowledge This book is useful for every enthusaist hacker and an eperienced hacker Here are just few of the topics that you are going to learn in this book 1) Introduction and Installation ofKali Linux What is Penetration Testing? How to Download Kali Linux Image file? Virtual Machine Installation of

Kali Linux Physical Machine Installation of Kali Linux Hard Disk Partition Explained Kali Linux Introduction How to use Kali Linux? Introduction to GUI and Commands in Kali Linux Complete Understanding of Settings Panel in Kali 2) Reconoissance for Hackers Introduction to Networking Information Gathering Principles How to Scan hosts and Ports? How to do domain analysis and Find subdomains? Finding services and Operating systems AnalysingGathered Information Complete understanding about Nmap 3) Scanning and Sniffing What are Vulnerabilities? Using Nessus to Scan Vulnerabilities Using OpenVAS to scan vulnerabilities Understanding Sniffing Monitoring Network Data 4) Metasploit Exploit Development Using Metasploit Understanding Meterpreter Exploit Binding Pdf Attacking 5) Password Cracking Wireless Network hacking Hacking Passwords by Bruteforcing and a lot more..... What are you waiting for? Go and Buy this book and Get Introduced to the world of hacking

Intermediate Security Testing with Kali Linux 2 - Daniel W. Dieterle 2015-09-25

Kali Linux 2 is the most advanced and feature rich penetration testing platform available. This hands-on learn by doing book will help take you beyond the basic features of Kali into a more advanced understanding of the tools and techniques used in security testing. If you have a basic understanding of Kali and want to learn more, or if you want to learn more advanced techniques, then this book is for you.Kali Linux is an Ethical Hacking platform that allows good guys to use the same tools and techniques that a hacker would use so they can find and correct security issues before the bad guys detect them. As a follow up to the popular "Basic Security Testing with Kali Linux" book, this work picks up where the first left off. Topics Include What is new in Kali 2? New Metasploit Features and Commands Creating Shells with Msfvenom Post Modules & Railgun PowerShell for Post Exploitation Web Application Pentesting How to use Burp Suite Security Testing Android Devices Forensics Tools for Security Testing Security Testing an Internet of Things (IoT) Device And much more!

Hacking with Kali Linux - Ged Holden 2021-12-12

Do you want to learn more about hacking and how to utilize these tactics to protect yourself and your network as secure as possible? Would you want to work with Kali Linux to defend your network and ensure that hackers cannot get access to your computer and inflict harm or steal your personal information? Have you ever wanted to understand more about the hacking process, how to prevent being taken advantage of, and how to use some of the tactics to your own needs? This manual will teach us all we need to know about hacking using Linux. Many individuals are concerned that hacking is a dangerous activity and that it is not the best solution for them. The good news is that hacking may be useful not just for stealing information and causing damage to others but also for assisting you in keeping your own network and personal information as secure as possible. Inside this guide, we'll look at the world of hacking and why the Kali Linux system is one of the finest for getting the job done. We discuss the many sorts of hacking and why it is useful to master some of the strategies required to execute your own hacks and get the desired effects with your own networks. In this guide, we will look at a variety of themes and methods that we will need to know while dealing with hacking on the Linux system. Some of the subjects we will look at here are as follows: The many sorts of hackers we may confront, as well as how they are similar and distinct. To get started, learn how to install Kali Linux on your operating system. The fundamentals of cybersecurity, online security, and cyberattacks, as well as how they might damage your computer system and how a hacker can attempt to exploit you. The many sorts of malware that hackers might use against you. A man in the middle, DoS, Trojans, viruses, and phishing are all hacker tools. And much, much more!..... Most individuals will not contemplate hacking because they are afraid it will be wicked or that it will only be used to hurt others. However, as we shall see in this manual, there is a lot more to the procedure than this. When you're ready to learn more about Kali Linux hacking and how it may help your own network and computer, check out our manual to get started!

Improving Your Penetration Testing Skills - Gilberto Najera-Gutierrez 2019-06-18

HACKING WITH KALI LINUX - Finn Loughran 2021-02-17

Would you like to learn professional hacking techniques? Would you like to learn advanced methods and strategies quickly? Now it is possible thanks to this detailed Book. The Ultimate Guide to Computer Hacking for beginners! In: "Hacking with Kali Linux: Step-By-Step beginner's Guide to Learn Hacking with Kali Linux and the Basics of Cyber Security with Penetration Testing & Wireless Hacking", leads you on a personal journey to understand how the process of Hacking works. You will be guided step by step, starting from the basics to get to the advanced processes. And you will have the capacity to understand how attackers gain access to your systems and steal information. Also, you will learn what you need to do to protect yourself from all kinds of hacking techniques. The skills acquired through this guide are for personal use, for the applications and methods permitted by law. Structured on 25 chapters, all about hacking, this is in short what the book covers in its pages: -Benefits of Kali Linux -The basics of CyberSecurity -How to install and use Kali Linux -Wireless Hotspot Security -iPhone Hacks & Software -The type of hackers -WordPress Security & Hacking -How the process of Hacking works and how attackers cover their traces -How to do Google Hacking -What's the role of a firewall and what are your firewall options -What you need to know about cryptography and digital signatures -What is a VPN and how to use it for your security -And much more! If you want to learn more about hacking, then this book will provide you with detailed information as well as other resources you can learn from. Start today and become an ethical hacker.

Web Penetration Testing with Kali Linux - Joseph Muniz 2013-09-25

Web Penetration Testing with Kali Linux contains various penetration testing methods using BackTrack that will be used by the reader. It contains clear step-by-step instructions with lot of screenshots. It is written in an easy to understand language which will further simplify the understanding for the user."Web Penetration Testing with Kali Linux" is ideal for anyone who is interested in learning how to become a penetration tester. It will also help the users who are new to Kali Linux and want to learn the features and differences in Kali versus Backtrack, and seasoned penetration testers who may need a refresher or reference on new tools and techniques. Basic familiarity with web-based programming languages such as PHP, JavaScript and MySQL will also prove helpful.

Kali Linux - Ethan Thorpe 2020-02-13

Are businesses run by organizations all about generating revenue, or there are more aspects to it? Have you wondered about how organizations today secure huge amounts of data they have about their customers? Have you thought about the effort that an organization puts in to securing data that is sensitive? Does this data include information about both the organization and the customer? Are you a data security enthusiast who wants to know about the process of securing data and wants to learn more about the security domain? Are you an aspiring IT Security professional, an Ethical Hacker, or a Penetration Tester? If you answered yes to all those questions, this is the book for you. This book will take you on a journey through the penetration testing life cycle using the most advanced tool available today, Kali Linux. You will learn about the five stages of penetration testing life cycle: Reconnaissance, Scanning, Exploitation, Maintaining Access, and Reporting and learn about the most common Kali Linux tools that can be utilized in all these stages. This book is for you if you are a technical professional who can benefit from knowing how penetration testers work. You will gain knowledge about the techniques used by penetration testers, which you could further use to make your systems secure. The knowledge in this book is not limited to developers, server admins, database admins, or network admins. You could transition from being a technical professional to a professional penetration tester by reading through this book, which will give you all the information you need. The knowledge that you already possess as a technical expert will give you the advantage of learning about penetration testing and Kali Linux in no time. The book will take you through examples that give you a step by step guide to using Kali Linux tools in all the five stages of the penetration testing life cycle. By trying out these examples by setting up your own Kali Linux system (which you already did in book one), you will be on your way to becoming a Penetration Tester. Throughout this book, you will gather information on the following: How do firewalls work in Kali Linux? How does the hacking process work? An introduction to Reconnaissance An introduction to Scanning Applications used in reconnaissance and scanning An introduction to Exploitation Applications and techniques used in exploitation How do you continue to maintain access into the system? What is reporting and the different tools used in reporting If you are an aspiring security engineer, the understanding of penetration testing will help you make your systems at home or your organization ever more secure. It will help you broaden your thought process and let you foresee how an attacker sees things in an information system. However, do note that if you are someone who is trying to penetrate the National Security Agency or a bank, this book is not for you. We also do

not recommend the book for security professionals who have been working on penetration testing and Kali Linux for a considerable number of years in their career. Our book is not for anyone who intends to break the law with the knowledge provided, and our objective is to introduce people to penetration testing as a way to make information systems more and more secure.
Learn Kali Linux 2019 - Glen D. Singh 2019-11-15

Kali Linux - Craig Berg 2019-08-29
You are about to discover how to start hacking with the #1 hacking/penetration testing tool, Kali Linux, in no time, even if you've never hacked before! Kali Linux is the king of all penetration testing tools out there. But while its 600+ pre-installed tools and utilities are meant to make penetration testing and forensics easy, at first, it can be overwhelming for experienced and aspiring security professionals to decide which tool to use to conduct a specific penetration test. That's where this book comes in to streamline your learning experience! If you are uncertain about where to begin even after reading and watching tons of free information online, this book will give you the much needed structure to go all in into the world of ethical hacking into secure computer systems with the best tool for the job. Since its introduction in 2012 as a successor to the previous version, Back Track Linux, Kali Linux has grown in popularity and capabilities to become the go-to open source security tool for information security professionals around the world. And this book will show you how to use it like the pros use it even if you've never stepped into a formal Kali Linux class before! In this book, we are going to cover the major features & tools provided by Kali Linux, including: Downloading, installation and set up Information gathering tools Vulnerability assessment Wireless attacks Web application attacks Exploitation tools Forensics tools Sniffing and spoofing Password cracking Maintaining access Social engineering tools Reverse engineering tools Hardware hacking tools Reporting tools Denial of service attacks And much more! We shall cover each of these features & tools individually so that after reading this guide, you have hands-on experience with using Kali Linux and can use what you learn when completing the hands-on Kali Linux practice project found in the part 17 of this guide. To make the learning experience faster and easier for you, for this hands-on, Kali Linux guide, we may have to install some other tools needed to make it easier to learn how to use Kali Linux for penetration testing and cyber security forensics. Everything is laid out with easy to follow examples and illustrations to help you to follow through, practice and ultimately remember whatever you are learning! What are you waiting for? Click Buy Now In 1-Click or Buy Now at the top of this page to get started!
Penetration Testing with Kali Linux - Pranav Joshi 2021-07-31
Perform effective and efficient penetration testing in an enterprise scenario KEY FEATURES ● Understand the penetration testing process using a highly customizable modular framework. ● Exciting use-cases demonstrating every action of penetration testing on target systems. ● Equipped with proven techniques and best practices from seasoned pen-testing practitioners. ● Experience-driven from actual penetration testing activities from multiple MNCs. ● Covers a distinguished approach to assess vulnerabilities and extract insights for further investigation. DESCRIPTION This book is designed to introduce the topic of penetration testing using a structured and easy-to-learn process-driven framework. Understand the theoretical aspects of penetration testing and create a penetration testing lab environment consisting of various targets to learn and practice your skills. Learn to comfortably navigate the Kali Linux and perform administrative activities, get to know shell scripting, and write simple scripts to effortlessly run complex commands and automate repetitive testing tasks. Explore the various phases of the testing framework while practically demonstrating the numerous tools and techniques available within Kali Linux. Starting your journey from gathering initial information about the targets and performing enumeration to identify potential weaknesses and sequentially building upon this knowledge to refine the attacks and utilize weaknesses to fully compromise the target machines. The authors of the book lay a particularly strong emphasis on documentation and the importance of generating crisp and concise reports which keep the various stakeholders' requirements at the center stage. WHAT YOU WILL LEARN ● Understand the Penetration Testing Process and its various phases. ● Perform practical penetration testing using the various tools available in Kali Linux. ● Get to know the process of Penetration Testing and set up the Kali Linux virtual environment. ● Perform active and passive reconnaissance. ● Learn to execute deeper analysis of vulnerabilities and extract exploit codes. ● Learn to solve challenges while performing penetration testing with expert tips. WHO THIS BOOK IS FOR This book caters to all IT professionals with a basic understanding of operating systems, networking, and Linux can use this book to build a skill set for performing real-world penetration testing. TABLE OF CONTENTS 1. The Basics of Penetration Testing 2. Penetration Testing Lab 3. Finding Your Way Around Kali Linux 4. Understanding the PT Process and Stages 5. Planning and Reconnaissance 6. Service Enumeration and Scanning 7. Vulnerability Research 8. Exploitation 9. Post Exploitation 10. Reporting
Learn Kali Linux 2019 - Glen D. Singh 2019-11-14
Explore the latest ethical hacking tools and techniques in Kali Linux 2019 to perform penetration testing from scratch Key FeaturesGet up and running with Kali Linux 2019.2Gain comprehensive insights into security concepts such as social engineering, wireless network exploitation, and web application attacksLearn to use Linux commands in the way ethical hackers do to gain control of your environmentBook Description The current rise in hacking and security breaches makes it more important than ever to effectively pentest your environment, ensuring endpoint protection. This book will take you through the latest version of Kali Linux and help you use various tools and techniques to efficiently deal with crucial security aspects. Through real-world examples, you'll understand how to set up a lab and later explore core penetration testing concepts. Throughout the course of this book, you'll get up to speed with gathering sensitive information and even discover different vulnerability assessment tools bundled in Kali Linux 2019. In later chapters, you'll gain insights into concepts such as social engineering, attacking wireless networks, exploitation of web applications and remote access connections to further build on your pentesting skills. You'll also focus on techniques such as bypassing controls, attacking the end user and maintaining persistence access through social media. Finally, this pentesting book covers best practices for performing complex penetration testing techniques in a highly secured environment. By the end of this book, you'll be able to use Kali Linux to detect vulnerabilities and secure your system by applying penetration testing techniques of varying complexity. What you will learnExplore the fundamentals of ethical hackingLearn how to install and configure Kali LinuxGet up to speed with performing wireless network pentestingGain insights into passive and active information gatheringUnderstand web application pentesting Decode WEP, WPA, and WPA2 encryptions using a variety of methods, such as the fake authentication attack, the ARP request replay attack, and the dictionary attackWho this book is for If you are an IT security professional or a security consultant who wants to get started with penetration testing using Kali Linux 2019.2, then this book is for you. The book will also help if you're simply looking to learn more about ethical hacking and various security breaches. Although prior knowledge of Kali Linux is not necessary, some understanding of cybersecurity will be useful.
Hacking with Kali Linux - Andrew Sutherland 2020-11
Are you interested in learning how to become a hacker? If your answer is yes, then look no further. This book will take you down that road! This book is going to teach you how hackers reason. Besides understanding the reasons why a hacker would target your computer, you will also get to know how they are able to do it and even how you can safeguard your systems, equipment, and network against hacking attacks. Keen readers will, by the end of this book understand how their systems work, how to scan, and how to gain access to your computer. The book has been structured into 11 chapters that will each teach you something new in matters hacking with Kali Linux. The formatting of the book is designed in a fashion that makes it simple to read and easy to understand. Concepts have been simplified to limit misunderstanding and enhance possibilities. By the time you come to the end of this book, you will have mastered the basics of computer hacking alongside a number of advanced concepts in social engineering attack mechanisms. The book is truly a template for everyone who intends to understand hacking. Additionally, you can expect the following from this book: Introduction to Kali Linux The Basics of Hacking and Using Kali Linux Kali Tools Penetration Testing The process of ethical hacking How to scanning devices in a network What are cyber-attacks? The basics of cybersecurity Vulnerability assessments Wireless network hacking Analyzing and managing networks Penetration Testing Web Security Text Manipulation Bash Scripting Cracking Encryptions Attacking with Frame Networks File systems Storage Device Management Becoming Secure and Anonymous Advanced Social Engineering Python scripting basics for hackers ..and Much More! Plenty of books about Hacking with Kali Linux

do not cover crucial concepts in a satisfactory fashion. Let me say again that nothing has been left out of this book. Grab yourself a copy of this book NOW, and you will get to discover interesting stuff about hacking using Kali Linux. The book will provide you a platform to be better a student, security administrator, or penetration tester. You will also find out how you can protect your computer from all the hacker's attacks!

Kali Linux Revealed - Raphaël Hertzog 2017-06-05

Whether you're a veteran or an absolute n00b, this is the best place to start with Kali Linux, the security professional's platform of choice, and a truly industrial-grade, and world-class operating system distribution-mature, secure, and enterprise-ready.

Kali Linux - Ethan Thorpe 2020-03-15

Manuscript 1: Kali Linux is believed to be amongst the best open-source security packages, which can be used by an ethical hacker. It consists of different sets of tools, which are divided into various categories. The user can install it as an operating system in the machine. The applications of Kali Linux have certainly evolved since it was first developed. Now, it is not only the best platform available for an information security professional, but it has become an industrial-level operation system distribution. In this book, you will learn about -The basics of Kali Linux-How to install Kali Linux-Steps to download Kali Linux-About ARM devices-Tips for troubleshooting-The applications and use of Kali Linux-Different tools available in Kali Linux, and much more! Manuscript 2: The book contains a practical approach to understand the different aspects of Kali Linux. It starts with a basic introduction to Kali Linux, followed by understanding how the hacking process works, and then understanding cybersecurity concept. With this core understanding, we then move to how Kali Linux is connected with Debian. To help new beginners, we also cover Linux Fundamentals. Next, our focus completely changes to what Kali Linux offers. We learn about Kali Linux configuration, documentation, community, security, monitoring, security assessment, and tools.In this book, you will learn the following: -Kali Linux introduction and installation-Introduction to hacking and hacking process-Learning cybersecurity concepts-Linux fundamentals refresh-Kali Linux configuration-Kali Linux Documentation and Community-Debian Package Management-Kali Linux Security Assessment-Kali Linux Tools-Network ScanningManuscript 3: This book is for you if you are a technical professional who can benefit from knowing how penetration testers work. You will gain knowledge about the techniques used by penetration testers, which you could further use to make your systems secure. The knowledge in this book is not limited to developers, server admins, database admins, or network admins. You could transition from being a technical professional to a professional penetration tester by reading through this book, which will give you all the information you need. The knowledge that you already possess as a technical expert will give you the advantage of learning about penetration testing and Kali Linux in no time. The book will take you through examples that give you a step by step guide to using Kali Linux tools in all the five stages of the penetration testing life cycle. By trying out these examples by setting up your own Kali Linux system (which you already did in book one), you will be on your way to becoming a Penetration Tester. Throughout this book, you will gather information on the following: -How do firewalls work in Kali Linux? -How does the hacking process work? -An introduction to Reconnaissance-An introduction to Scanning-Applications used in reconnaissance and scanning-An introduction to Exploitation-Applications and techniques used in exploitation-How do you continue to maintain access into the system? -What is reporting and the different tools used in reportingIf you are an aspiring security engineer, the understanding of penetration testing will help you make your systems at home or your organization ever more secure. It will help you broaden your thought process and let you foresee how an attacker sees things in an information system.

Hacking with Kali Linux - Alan Harrett 2021-11-21

Do you want to become a skilled cybersecurity professional and master the foundations of ethical hacking? Do you want a full breakdown of all the fundamental tools supplied by the finest Linux distribution for ethical hacking? Have you combed the internet for the right resource to help you get started with hacking, only to be overwhelmed by the quantity of contradictory material available on the subject of hacking and cybersecurity? If you answered yes to any of these questions, this book is for you. Hacking is growing more sophisticated and complicated, and businesses are trying to secure their digital assets from dangers by implementing cybersecurity measures. These systems must be reviewed on a regular basis to verify that they are performing as intended. Penetration testers and ethical hackers, programmers who are educated to detect and exploit network flaws and suggest solutions to cover them up, are the individuals who can do these inspections. Companies are searching for penetration testers and cybersecurity specialists that have actual, hands-on expertise with Kali Linux and other open-source hacking tools now more than ever. This powerful book will teach you how to master the industry-standard platform for hacking, penetration testing, and security testing. This book assumes you know nothing about Kali Linux or hacking. It will teach you from the ground up how to utilize Kali Linux and other open-source tools to become a hacker and understand the procedures behind a successful penetration test. Here's a sneak peek at what you'll study in Kali Linux Hacking: A brief overview of the notion of "hacking" and Kali Linux. Everything you need to know about hacking, from session hijacking and SQL injection to phishing and denial-of-service assaults. Why hackers aren't necessarily terrible folks, as well as the eight different sorts of hackers in today's world Why is Kali Linux so popular among both amateur and professional hackers? Step-by-step instructions for installing and configuring Kali Linux on your PC. How to grasp the Linux terminal, as well as basic Linux commands you must be aware with An in-depth look at how to use Nmap to analyze, discover, and exploit vulnerabilities. How to remain anonymous when conducting hacking assaults or penetration testing How to Become a Better Hacker by Using Bash and Python Scripting ...and Much More!.... This book is intended for total novices and is jam-packed with practical examples and real-world hacking methods taught in clear, straightforward English. This book is for the next generation of 21st-century hackers and cyber defenders, and it will help you improve your cybersecurity and pen-testing abilities. Whether you're just starting with hacking, planning for a career transition into the realm of cybersecurity, or just trying to beef up your résumé and make yourself more appealing to recruiters, Kali Linux Hacking is the book for you! Do you want to learn more? To get started, click Buy Now With 1-Click or Buy Now.

Cyber Security - Zach Codings 2019-10-20

How do I secure my computer? What is malware and how do I get rid of it? Do I only need to worry about Phishing attacks via email? What if my personal email account, bank account, or other accounts were compromised? Sounds familiar? Keep reading... Cybersecurity has changed significantly in the past decade, we've moved away from the days when basic virus protection and security controls were sufficient to deter threats, to the need for advanced security analytics tools to prevent advanced persistent threats (APTs) and tackle malicious insiders. This book includes: Hacking with Kali Linux: A Beginner's Guide to Learn Penetration Testing to Protect Your Family and Business from Cyber Attacks Building a Home Security System for Wireless Network Security Here's a sneak peek of what you'll learn with this book: What is hacking The importance of cybersecurity How malware and cyber-attacks operate How to install Kali Linux on a virtual box How to scan networks VPNs & Firewalls An introduction to Digital Signatures and Cryptography and much more... Ethical Hacking: A Beginner's Guide to Computer and Wireless Networks Defense Strategies, Penetration Testing and Information Security Risk Assessment Throughout these pages, you will learn: Roles and responsibilities of an Ethical Hacker Hacking as a career Making money freelance Most common security tools The three ways to scan your system The seven proven penetration testing strategies and much more... Even if you aren't a security expert, there are a few basic steps you can take to secure your computer. Arm yourself with all this knowledge! Scroll up and click the BUY NOW BUTTON!

Einstieg in Kali Linux - Jürgen Ebner 2021-11-23

• Von der Installation über die Konfiguration bis hin zum Einsatz der wichtigsten Tools • Detaillierter Ablauf von Security Assessments und Durchführung von Penetrationstests mit praktischer Checkliste • Schwachstellenanalyse mit OpenVAS, Angriffe mit WebScarab und Metasploit, IT-Forensik mit Autopsy, Reporting mit Faraday und viele weitere Tools Die Distribution Kali Linux ist auf Sicherheits- und Penetrationstests spezialisiert. Sie enthält mehrere Hundert Pakete zur Informationssammlung und Schwachstellenanalyse und jede Menge Tools für Angriffe und Exploitation sowie Forensik und Reporting, sodass Penetration Tester aus einem beinahe endlosen Fundus kostenloser Tools schöpfen können. Dieses Buch ermöglicht IT-Sicherheitsexperten und allen, die es werden wollen, einen einfachen Einstieg in Kali Linux. Erfahrung im Umgang mit anderen Linux-Distributionen setzt der Autor dabei nicht voraus. Im ersten Teil des Buches erfahren Sie, wie Sie Kali Linux installieren und an Ihre Bedürfnisse anpassen. Darüber hinaus gibt Ihnen der Autor grundlegende Linux-Kenntnisse an die Hand, die Sie für das Penetration Testing mit Kali Linux brauchen. Der zweite Teil erläutert verschiedene Security Assessments sowie die grundlegende

Vorgehensweise bei der Durchführung von Penetrationstests. So vorbereitet können Sie im nächsten Schritt gezielt die für Ihren Einsatzzweck passenden Tools für das Penetration Testing auswählen. Aus der Fülle der bei Kali Linux mitgelieferten Tools stellt der Autor im dritten Teil des Buches die wichtigsten vor und zeigt Schritt für Schritt, wie und wofür sie eingesetzt werden, darunter bekannte Tools wie Nmap, OpenVAS, Metasploit und John the Ripper. Nach der Lektüre sind Sie bereit, Kali Linux sowie die wichtigsten mitgelieferten Tools für Penetrationstests einzusetzen und IT-Systeme auf Schwachstellen zu prüfen. Aus dem Inhalt: • Hauptfeatures und Richt-linien von Kali Linux • Installation und Konfiguration • Linux-Dateisystem, Kommandozeile und nützliche Linux-Befehle • Sicherheitsrichtlinien • Einführung in Security Assessments • Durchführung von Pentests • Informationssammlung • mit Nmap, TheHarvester, HTTrack u.v.m. • Schwachstellenanalyse mit OpenVAS, Nikto und Siege • Sniffing und Spoofing mit Dsniff, Ettercap und Wireshark • Tools für Attacken: Wireless-Attacken (aircrack-ng, Ghost Phisher, Kismet) • Pentesting von Webseiten (WebScarab, Skipfish, ZAP) • Exploitation (Metasploit, Armitage u.v.m.) • Passwort-Angriffe (Medusa, JtR u.v.m.) • IT-Forensik mit Autopsy, Binwalk und mehr • Reporting mit Cutycapt, Faraday und mehr • Checkliste für Penetrationstests • Praktisches Glossar

A Beginners Guide to Kali Linux - Michael Smith 2020-12-05

Kali Linux The truth is: Kali Linux is an open-source project which is maintained and funded by Offensive Security. It provides state-of-the-art information security training and penetration testing services. Do you want to know more about Kali Linux? Do you want to increase your knowledge about Kali Linux? Read On... It is a Debian-based Linux distribution which aims at advanced penetration Testing and Security Auditing. There are various tools in Kali which look after information security tasks like Security Research, Computer Forensics, Penetration Testing and Reverse Engineering. Released on 13th March, 2013, it is a comprehensive rebuild of the BackTrack Linux, maintaining the Debian development standards. Kali Linux includes more than 600 penetration testing tools. There were many tools in backtrack which needed a review as some of them did not work whereas the others were a duplicate of the tools having similar functions. The tools are completely free of charge and all the source code going into Kali Linux is available for everyone who wants to customize the packages to suit their specific needs. Kali also adheres to the File system Hierarchy Standard allowing the Linux users in easy location of binaries, supporting the libraries and the files etc. DOWNLOAD: A Beginner's Guide to Kali Linux, The step by Step Guide for Beginners to Install and Learn the Essentials Hacking Command Line. Learning All the Basic of Kali Linux and How to Use It For Hacking. The goal of the eBook is simple: The eBook helps in knowing more about Kali Linux. Most of the penetration tools are written in English but Kali includes a multilingual approach. This makes it accessible to a greater number of users who can operate it in their own language. They can also locate the tools which are needed for their job. You Will Also Learn: - The basic of Kali Linux - Step by step guide on how to install and download - Uses and applications of Kali Linux - List of all uses with applications - How scanning of devices in a network works - Learning the essential hacking command line - How Linux commands can be used in hacking 1. Use 1 2. Examples of uses - Customizing Kali Linux Would you like to know more? Download the eBook, A Beginner's Guide to Kali Linux to have an idea about a useful tool. Scroll to the top of the page and select the buy now button.

Kali Linux Hacking - Ethem Mining 2019-12-10

Do you want to become a proficient specialist in cybersecurity and you want to learn the fundamentals of ethical hacking? Do you want to have a detailed overview of all the basic tools provided by the best Linux distribution for ethical hacking? Have you scoured the internet looking for the perfect resource to help you get started with hacking, but became overwhelmed by the amount of disjointed information available on the topic of hacking and cybersecurity? If you answered yes to any of these questions, then this is the book for you. Hacking is becoming more complex and sophisticated, and companies are scrambling to protect their digital assets against threats by setting up cybersecurity systems. These systems need to be routinely checked to ensure that these systems do the jobs they're designed to do. The people who can do these checks are penetration testers and ethical hackers, programmers who are trained to find and exploit vulnerabilities in networks and proffer ways to cover them up. Now more than ever, companies are looking for penetration testers and cybersecurity professionals who have practical, hands-on experience with Kali Linux and other open-source hacking tools. In this powerful book, you're going to learn how to master the industry-standard platform for hacking, penetration and security testing--Kali Linux. This book assumes you know nothing about Kali Linux and hacking and will start from scratch and build up your practical knowledge on how to use Kali Linux and other open-source tools to become a hacker as well as understand the processes behind a successful penetration test. Here's a preview of what you're going to learn in Kali Linux Hacking: A concise introduction to the concept of "hacking" and Kali Linux Everything you need to know about the different types of hacking, from session hijacking and SQL injection to phishing and DOS attacks Why hackers aren't always bad guys as well as the 8 hacker types in today's cyberspace Why Kali Linux is the platform of choice for many amateur and professional hackers Step-by-step instructions to set up and install Kali Linux on your computer How to master the Linux terminal as well as fundamental Linux commands you absolutely need to know about A complete guide to using Nmap to understand, detect and exploit vulnerabilities How to effectively stay anonymous while carrying out hacking attacks or penetration testing How to use Bash and Python scripting to become a better hacker ...and tons more! Designed with complete beginners in mind, this book is packed with practical examples and real-world hacking techniques explained in plain, simple English. This book is for the new generation of 21st-century hackers and cyber defenders and will help you level up your skills in cybersecurity and pen-testing. Whether you're just getting started with hacking or you're preparing for a career change into the field of cybersecurity, or are simply looking to buff up your resume and become more attractive to employers, Kali Linux Hacking is the book that you need! Would You Like To Know More? Click Buy Now With 1-Click or Buy Now to get started!

Hacking und IT-Security für Einsteiger - Max Engelhardt 2020

Kali Linux - Ethan Thorpe 2019-12-16

The Kali Linux book is a beginner's introduction to Kali Linux. In today's world, security is one of the most important talks of the town. It is necessary to secure the infrastructure that powers the world around us. Kali Linux aids in the vision of a secure world where everything is connected. It is a penetration testing operating system used by professionals all around the world. The book can be used by anyone who has an interest in Linux, Hacking, Security, Pentesting, and others, and will act as a good starting point to work with Kali Linux. After reading this book, you will be able to work optimally with Kali Linux and make the most out of what Kali Linux has to offer. The book contains a practical approach to understand the different aspects of Kali Linux. It starts with a basic introduction to Kali Linux, followed by understanding how the hacking process works, and then understanding cybersecurity concept. With this core understanding, we then move to how Kali Linux is connected with Debian. To help new beginners, we also cover Linux Fundamentals. Next, our focus completely changes to what Kali Linux offers. We learn about Kali Linux configuration, documentation, community, security, monitoring, security assessment, and tools. In this book, you will learn the following: Kali Linux introduction and installation Introduction to hacking and hacking process Learning cybersecurity concepts Linux fundamentals refresh Kali Linux configuration Kali Linux Documentation and Community Debian Package Management Kali Linux Security Assessment Kali Linux Tools Network Scanning All the topics are covered in-depth to enhance your knowledge. By reading the book, you will be able to use Kali Linux as your daily driver and understand what makes it so awesome!

Mastering Kali Linux Wireless Pentesting - Jilumudi Raghu Ram 2016-02-25

Test your wireless network's security and master advanced wireless penetration techniques using Kali Linux About This Book Develop your skills using attacks such as wireless cracking, Man-in-the-Middle, and Denial of Service (DOS), as well as extracting sensitive information from wireless networks Perform advanced wireless assessment and penetration tests Use Embedded Platforms, Raspberry PI, and Android in wireless penetration testing with Kali Linux Who This Book Is For If you are an intermediate-level wireless security consultant in Kali Linux and want to be the go-to person for Kali Linux wireless security in your organisation, then this is the book for you. Basic understanding of the core Kali Linux concepts is expected. What You Will Learn Fingerprint wireless networks with the various tools available in Kali Linux Learn various techniques to exploit wireless access points using CSRF Crack WPA/WPA2/WPS and crack wireless encryption using Rainbow tables more quickly Perform man-in-the-middle attack on wireless clients Understand client-side attacks, browser exploits, Java vulnerabilities, and

social engineering Develop advanced sniffing and PCAP analysis skills to extract sensitive information such as DOC, XLS, and PDF documents from wireless networks Use Raspberry PI and OpenWrt to perform advanced wireless attacks Perform a DOS test using various techniques and tools In Detail Kali Linux is a Debian-based Linux distribution designed for digital forensics and penetration testing. It gives access to a large collection of security-related tools for professional security testing - some of the major ones being Nmap, Aircrack-ng, Wireshark, and Metasploit. This book will take you on a journey where you will learn to master advanced tools and techniques to conduct wireless penetration testing with Kali Linux. You will begin by gaining an understanding of setting up and optimizing your penetration testing environment for wireless assessments. Then, the book will take you through a typical assessment from reconnaissance, information gathering, and scanning the network through exploitation and data extraction from your target. You will get to know various ways to compromise the wireless network using browser exploits, vulnerabilities in firmware, web-based attacks, client-side exploits, and many other hacking methods. You will also discover how to crack wireless networks with speed, perform man-in-the-middle and DOS attacks, and use Raspberry Pi and Android to expand your assessment methodology. By the end of this book, you will have mastered using Kali Linux for wireless security assessments and become a more effective penetration tester and consultant. Style and approach This book uses a step-by-step approach using real-world attack scenarios to help you master the wireless penetration testing techniques.

Kali Linux for Hackers - Karnel Erickson 2020-10-29

Do you want to know how to protect your system from being compromised and learn about advanced security protocols? Do you want to improve your skills and learn how hacking actually works? If you want to understand how to hack from basic level to advanced, keep reading... A look into the box of tricks of the attackers can pay off, because who understands how hacking tools work, can be better protected against attacks. Kali-Linux is popular among security experts, which have various attack tools on board. It allows you to examine your own systems for vulnerabilities and to simulate attacks. This book introduces readers by setting up and using the distribution and it helps users who have little or no Linux experience.. The author walks patiently through the setup of Kali-Linux and explains the procedure step by step. This practical, tutorial-style book uses the Kali Linux distribution to teach Linux basics with a focus on how hackers would use them. Topics includes Network security WLAN VPN WPA / WPA2 WEP Nmap and OpenVAS Attacks Linux tools Solving level problems Exploitation of security holes And more... "Kali Linux for Hackers" will help you understand the better use of Kali Linux and it will teach you how you can protect yourself from most common hacking attacks. You will stay a step ahead of any criminal hacker! So let's start now, order your copy today!Scroll to the top of the page and select the buy now button. Buy paperback format and receive for free the kindle version!