How To Install Kali Linux On Raspberry Pi3 Complete Step By Step Picture Guide On How To Setup And Kali Linux On Raspberry Pi3 In Less Than 1 Hour For Complete Beginners

Achieve the gold standard in penetration testing with Kali using this masterpiece, now in its third edition! About This Book Get a rock-solid insight into penetration testing techniques and test your corporate network against threats like never before Formulate your pentesting strategies by relying on the most up-to-date and feature-rich Kali version in town—Kali Linux 2 (aka Sana). Experience this journey with new cutting-edge wireless penetration tools and a variety of new features to make your pentesting experience smoother Who This Book Is For If you are an IT security professional or a student with basic knowledge of Unix/Linux operating systems, including an awareness of information security factors, and you want to use Kali Linux for penetration testing, this book is for you. What You Will Learn Find out to download and install your own copy of Kali Linux Properly scope and conduct the initial stages of a penetration test Conduct reconnaissance and enumeration of target networks Exploit and gain a foothold on a target system or network Obtain and crack passwords Use the Kali

Linux NetHunter install to conduct wireless penetration testing Create proper penetration testing reports In Detail Kali Linux is a comprehensive penetration testing platform with advanced tools to identify, detect, and exploit the vulnerabilities uncovered in the target network environment. With Kali Linux, you can apply appropriate testing methodology with defined business objectives and a scheduled test plan, resulting in a successful penetration testing project engagement. Kali Linux – Assuring Security by Penetration Testing is a fully focused, structured book providing guidance on developing practical penetration testing skills by demonstrating cutting-edge hacker tools and techniques with a coherent, step-by-step approach. This book offers you all of the essential lab preparation and testing procedures that reflect real-world attack scenarios from a business perspective, in today's digital age. Style and approach This practical guide will showcase penetration testing through cutting-edge tools and techniques using a coherent, step-by-step approach.

Learn the skills you need to take advantage of Kali Linux for digital forensics investigations using this comprehensive guide Key Features Master powerful Kali Linux tools for digital investigation and analysis Perform evidence acquisition, preservation, and analysis using various tools within Kali Linux Implement the concept of cryptographic hashing and

imaging using Kali Linux Perform memory forensics with Volatility and internet forensics with Xplico. Discover the capabilities of professional forensic tools such as Autopsy and DFF (Digital Forensic Framework) used by law enforcement and military personnel alike Book Description Kali Linux is a Linux-based distribution used mainly for penetration testing and digital forensics. It has a wide range of tools to help in forensics investigations and incident response mechanisms. You will start by understanding the fundamentals of digital forensics and setting up your Kali Linux environment to perform different investigation practices. The book will delve into the realm of operating systems and the various formats for file storage, including secret hiding places unseen by the end user or even the operating system. The book will also teach you to create forensic images of data and maintain integrity using hashing tools. Next, you will also master some advanced topics such as autopsies and acquiring investigation data from the network, operating system memory, and so on. The book introduces you to powerful tools that will take your forensic abilities and investigations to a professional level, catering for all aspects of full digital forensic investigations from hashing to reporting. By the end of this book, you will have had hands-on experience in implementing all the pillars of digital forensics—acquisition, extraction, analysis, and

presentation using Kali Linux tools. What you will learn Get to grips with the fundamentals of digital forensics and explore best practices Understand the workings of file systems, storage, and data fundamentals Discover incident response procedures and best practices Use DC3DD and Guymager for acquisition and preservation techniques Recover deleted data with Foremost and Scalpel Find evidence of accessed programs and malicious programs using Volatility. Perform network and internet capture analysis with Xplico Carry out professional digital forensics investigations using the DFF and Autopsy automated forensic suites Who this book is for This book is targeted at forensics and digital investigators, security analysts, or any stakeholder interested in learning digital forensics using Kali Linux. Basic knowledge of Kali Linux will be an advantage.

Master the art of identifying vulnerabilities within the Windows OS and develop the desired solutions for it using Kali Linux. Key Features Identify the vulnerabilities in your system using Kali Linux 2018.02 Discover the art of exploiting Windows kernel drivers Get to know several bypassing techniques to gain control of your Windows environment Book Description Windows has always been the go-to platform for users around the globe to perform administration and ad hoc tasks, in settings that range from small offices to global enterprises,

and this massive footprint makes securing Windows a unique challenge. This book will enable you to distinguish yourself to your clients. In this book, you'll learn advanced techniques to attack Windows environments from the indispensable toolkit that is Kali Linux. We'll work through core network hacking concepts and advanced Windows exploitation techniques, such as stack and heap overflows, precision heap spraying, and kernel exploitation, using coding principles that allow you to leverage powerful Python scripts and shellcode. We'll wrap up with post-exploitation strategies that enable you to go deeper and keep your access. Finally, we'll introduce kernel hacking fundamentals and fuzzing testing, so you can discover vulnerabilities and write custom exploits. By the end of this book, you'll be well-versed in identifying vulnerabilities within the Windows OS and developing the desired solutions for them. What you will learn Get to know advanced pen testing techniques with Kali Linux Gain an understanding of Kali Linux tools and methods from behind the scenes See how to use Kali Linux at an advanced level Understand the exploitation of Windows kernel drivers Understand advanced Windows concepts and protections, and how to bypass them using Kali Linux Discover Windows exploitation techniques, such as stack and heap overflows and kernel exploitation, through coding principles Who this book is for This book is for

penetration testers, ethical hackers, and individuals breaking into the pentesting role after demonstrating an advanced skill in boot camps. Prior experience with Windows exploitation, Kali Linux, and some Windows debugging tools is necessary 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? Over 70 recipes for system administrators or DevOps to master Kali Linux 2 and perform effective security assessments About This Book Set up a penetration testing lab to conduct a preliminary assessment of attack surfaces and run exploits Improve your testing efficiency with the use of automated vulnerability scanners Work through step-by-step recipes to detect a wide array of vulnerabilities, exploit them to analyze their consequences, and identify security anomalies Who This Book Is For This book is intended for those who want to know more about information security. In particular, it's ideal for system administrators and system architects who want to ensure that the infrastructure and systems they are creating and managing are secure. This book helps both beginners and intermediates by allowing them to use it as a reference book and to gain in-depth

knowledge. What You Will Learn Understand the importance of security assessments over merely setting up and managing systems/processes Familiarize yourself with tools such as OPENVAS to locate system and network vulnerabilities Discover multiple solutions to escalate privileges on a compromised machine Identify security anomalies in order to make your infrastructure secure and further strengthen it Acquire the skills to prevent infrastructure and application vulnerabilities Exploit vulnerabilities that require a complex setup with the help of Metasploit In Detail With the increasing threats of breaches and attacks on critical infrastructure, system administrators and architects can use Kali Linux 2.0 to ensure their infrastructure is secure by finding out known vulnerabilities and safeguarding their infrastructure against unknown vulnerabilities. This practical cookbook-style guide contains chapters carefully structured in three phases – information gathering, vulnerability assessment, and penetration testing for the web, and wired and wireless networks. It's an ideal reference guide if you're looking for a solution to a specific problem or learning how to use a tool. We provide hands-on examples of powerful tools/scripts designed for exploitation. In the final section, we cover various tools you can use during testing, and we help you create in-depth reports to impress management. We provide system engineers with

steps to reproduce issues and fix them. Style and approach This practical book is full of easy-to-follow recipes with based on real-world problems faced by the authors. Each recipe is divided into three sections, clearly defining what the recipe does, what you need, and how to do it. The carefully structured recipes allow you to go directly to your topic of interest.

"Kali Linux is a Linux distribution designed for digital forensics, penetration testing, and security auditing. It is the successor of BackTrack, the world's most popular penetration testing distributor. Kali Linux includes many well-known security tools, and this course will teach you more about the tools and their usage. This course not only shows you how to install Kali Linux, but also how to properly plan the installation and select the best hardware. We'll include post-installation tasks and you'll see how to configure Kali Linux to get the best performance, as well as ensuring your project needs are satisfied. Within this, we'll show you how to gather information using the tools present in Kali Linux. The tools used in this course teach you how to acquire information about a target including web applications, documents, metadata, and other popular and powerful tools included with the distribution. This course helps you plan and install Kali Linux to get the optimal results for your specific needs. We'll emphasize how to choose the best hardware and

install the distribution and troubleshoot problems that may arise during the process. The course wraps up with post-installation and configuration tasks."--Resource description page.
this book Mastering Kali Linux for. Advanced Penetration Testing. A practical guide to testing your network's security with. Kali Linux, the preferred choice of penetration testers and hackers Kali Linux has not only become the information security professional's platform of choice, but evolved into an industrial-grade, and world-class operating system distribution--mature, secure, and enterprise-ready. Through the decade-long development process, Muts and his team, along with countless volunteers from the hacker community, have taken on the burden of streamlining and organizing our work environment, freeing us from much of the drudgery. They provided a secure and reliable foundation, allowing us to concentrate on securing our digital world. An amazing community has built up around Kali Linux. Every month, more than 300,000 of us download a version of Kali. We come together in online and real-world training rooms and grind through the sprawling Offensive Security Penetration Testing Labs, pursuing the near-legendary Offensive Security certifications. We come together on the Kali forums, some 40,000 strong, and hundreds of us at a time can be found on the Kali IRC channel. We gather at conferences and attend Kali Dojos to learn

from the developers themselves how to best leverage Kali. However, the Kali team has never released an official Kali Linux manual, until now. In this book, we'll focus on the Kali Linux platform itself, and help you understand and maximize Kali from the ground up. The developers will walk you through Kali Linux features and fundamentals, provide a crash course in basic Linux commands and concepts, and then walk you through the most common Kali Linux installation scenarios. You'll learn how to configure, troubleshoot and secure Kali Linux and then dive into the powerful Debian package manager. Throughout this expansive section, you'll learn how to install and configure packages, how to update and upgrade your Kali installation, and how to create your own custom packages. Then you'll learn how to deploy your custom installation across massive enterprise networks. Finally, you'll be guided through advanced topics such as kernel compilation, custom ISO creation, industrial-strength encryption, and even how to install crypto kill switches to safeguard your sensitive information. 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

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. 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 Quickstart guide for Hacking with Kali LinuxKali Linux is a an incredibly powerful and useful Linux distribution, but only if you know how to use it! Need to learn hacking with Kali Linux fast?Kali Linux can be used can be used for a wide variety of hacking, penetration testing, and

digital forensics projects. When you understand how hacking in Kali Linux works, you unlock a world of computing power and possibilities. Get the most out of Kali Linux simply by following the easy step by step coding examples and projects fully explained inside this guide. It doesn't matter if you have never installed a Linux distribution before. This step-by-step guide gives you everything you need to know to get hacking with Kali Linux!Fully up to date for 2019Kali Linux has been around for a while, but has evolved over the years. Save yourself the headache and frustration of trying to use a guide that just isn't up to date anymore! Brand new and fully up to date, this guide shows you exactly what you need to do to start hacking using Kali Linux today!Here is a preview of what you will learn in this guide: Kali Linux What is Hacking? What are the types of Hackers? What are some common hacker attacks? What is Ethical Hacking? What is Kali Linux? What is a Linux Distribution? Features of Kali Linux Why use Kali Linux Getting Started with Kali Linux Downloading Kali Linux Where to download Kali Linux Official Kali Linux Images Kali Linux ISO files for Intel - processor Personal Computers Kali Linux Images on VMware Kali Linux ARM Images Verifying Kali Linux Downloads GNU Privacy Guard (GPG) Building Your own Kali Linux ISO Preparing Kali Linux to set up the live - build system Configuring and Customizing the Kali Linux ISO Building Kali Linux Using Differing Desktop Environments Customizing the packages in your Kali Linux Build Build hooks, binary, and chroots Overlaying Build Files Building a Kali Linux ISO for older 32 - bit (i386) system

architecture Building Kali Linux on Non-Kali Debian Based Systems Setting up Kali Linux Installing Kali Linux on your hard disk drive Preliminary Requirements Installation Procedure Installing Kali Linux over a network (Preboot Execution Environment) Installing Kali Linux as an encrypted disk install Preliminary Requirements Installation Procedure Dual Booting Kali Linux and the Windows Operating System Creating a Partition Installation Procedure Hacking Using Kali Linux WiFi Hacking SQL Injection And so much more! If you aren't a tech-savvy person or have no hacking experience, have no fear! With this guide in your hands that will not be a barrier for you any longer. Learn how to hack using Kali Linux quickly and easily when you grab this guide now!

If you are looking for a low budget, small form-factor remotely accessible hacking tool, then the concepts in this book are ideal for you. If you are a penetration tester who wants to save on travel costs by placing a low-cost node on a target network, you will save thousands by using the methods covered in this book. You do not have to be a skilled hacker or programmer to use this book. It will be beneficial to have some networking experience; however, it is not required to follow the concepts covered in this book.

Convert Android to a powerful pentesting platform. Key Features Get 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 data Book 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 learn Choose 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 devices Who 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 is the most popular distribution dedicated to penetration testing that includes a set of free, open source tools. This book introduces you to wireless penetration testing and describes how to conduct its various phases. After showing you how to install Kali Linux on your laptop, you will verify the requirements of the wireless adapter and configure it. Next, the book covers the wireless LAN reconnaissance phase, explains the WEP and WPA/WPA2 security protocols and demonstrates practical attacks against them using the tools provided in Kali Linux, Aircrack-ng in particular. You will then discover the advanced and latest attacks targeting access points and wireless clients and learn how to create a professionally written and effective report.

Over 120 recipes to perform advanced penetration testing with Kali Linux About This Book Practical recipes to conduct effective penetration testing using the powerful Kali Linux Leverage tools like Metasploit, Wireshark, Nmap, and many more to detect vulnerabilities with ease Confidently perform networking and application attacks using task-oriented recipes Who

This Book Is For This book is aimed at IT security professionals, pentesters, and security analysts who have basic knowledge of Kali Linux and want to conduct advanced penetration testing techniques. What You Will Learn Installing, setting up and customizing Kali for pentesting on multiple platforms Pentesting routers and embedded devices Bug hunting 2017 Pwning and escalating through corporate network Buffer overflows 101 Auditing wireless networks Fiddling around with software-defned radio Hacking on the run with NetHunter Writing good quality reports In Detail With the current rate of hacking, it is very important 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 2016.2) according to your needs, and move on to core functionalities. This book will start with the installation and configuration of Kali Linux so that you can perform your tests. You will learn how to plan attack strategies and perform web application exploitation using tools such as Burp, and Jexboss. You will also learn how to perform network exploitation using Metasploit, Sparta, and Wireshark. Next, you will perform wireless and password attacks using tools such as Patator, John the Ripper, and airoscript-ng. Lastly, you will learn how to create an optimum quality pentest report! By the end of this book, you will know how to conduct advanced penetration testing thanks to the book's crisp and task-oriented recipes. Style and approach This is a recipe-based book that allows you to venture into some of the most cutting-edge practices and techniques to perform

penetration testing with Kali Linux.

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.

A practical, cookbook style with numerous chapters and recipes explaining the penetration testing. The cookbook-style recipes allow you to go directly to your topic of interest if you are an expert using this book as a reference, or to follow topics throughout a chapter to gain in-depth knowledge if you are a beginner.This book is ideal for anyone who wants to get up to speed with Kali Linux. It would also be an ideal book to use as a reference for seasoned penetration testers.

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.

If you want to learn how to use Linux and level up your career but are pressed for time, read on.As the founder of the Linux Training Academy and an instructor of several courses, I've had the good fortune of helping thousands of people hone their Linux skills. Interacting with so many people who are just getting started with the Linux operating system has given me invaluable insight into the particular struggles and challenges people face at this stage.One of the biggest challenges for people interested in learning the ins and outs of Linux is simply a lack of time. When you are working with a limited and extremely valuable resource you want to make sure you make the most of it.The next biggest challenge for Linux newcomers is knowing where to start. There is so much information available that deciding what to focus your attention on first is a big enough hurdle to keep many people from even starting. What's worse is starting down the path of learning only to discover too many concepts, commands, and nuances that aren't explained. This kind of experience is frustrating and leaves you with more questions than answers.That's why I've written this book.Not only have I condensed the most important material into five sections, each designed to be consumed in a day, I've also structured

the content in a logical and systematic manner. This way you'll be sure to make the most out of your time by learning the foundational aspects of Linux first and then building upon that foundation each day.In Learn Linux in 5 Days you will learn the most important concepts and commands, and be guided step-by-step through several practical and real-world examples. As new concepts, commands, or jargon are encountered they are explained in plain language, making it easy to understand.Here is what you will learn by reading Learn Linux in 5 Days: How to get access to a Linux server if you don't already. What a Linux distribution is and which one to choose. What software is needed to connect to Linux from Mac and Windows computers. Screenshots included. What SSH is and how to use it, including creating and using SSH keys. The file system layout of Linux systems and where to find programs, configurations, and documentation. The basic Linux commands you'll use most often. Creating, renaming, moving, and deleting directories. Listing, reading, creating, editing, copying, and deleting files. Exactly how permissions work and how to decipher the most cryptic Linux permissions with ease. How to use the nano, vi, and emacs editors. Two methods to search for files and directories. How to compare the contents of files. What pipes are, why they are useful, and how to use them. How to compress files to save space and make transferring data easy. How and why to redirect input and output from applications. How to customize your shell prompt. How to be efficient at the command line by using aliases, tab completion, and your shell history. How to schedule and automate jobs using cron. How to switch users and run processes as others. Where to go for even more in-depth coverage on each topic. What you learn in Learn Linux in 5 Days applies to any Linux environment including Ubuntu, Debian, Linux Mint, RedHat, Fedora, OpenSUSE, Slackware, and more.Scroll up, click the Buy Now With 1 Click button and

get started learning Linux today!

PYTHON INSTALLATION IN KALI LINUX

Discover end-to-end penetration testing solutions to enhance your ethical hacking skills Key Features Practical recipes to conduct effective penetration testing using the latest version of Kali Linux Leverage tools like Metasploit, Wireshark, Nmap, and more to detect vulnerabilities with ease Confidently perform networking and application attacks using task-oriented recipes Book 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 learn Learn how to install, set up and customize Kali for pentesting on multiple platforms Pentest routers and embedded devices Get insights into

fiddling around with software-defined radio Pwn and escalate through a corporate network Write good quality security reports Explore digital forensics and memory analysis with Kali Linux Who 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. Become an expert in Kali Linux within no time! Do you want to learn about Kali Linux? Do you want to improve your knowledge about advanced security protocols? However, you aren't sure where to begin? Does all the information available online seem overwhelming and quite complicated? If yes, then this is the perfect book for you. This book is a beginner's guide to learn Kali Linux. Armed with the information given in this book, you can use Kali Linux quite easily and become an expert in it within no time. 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! If you want to learn about all this, then this book is your go-to option. Now, all that's left for you to do is grab your copy today and start learning! What are you waiting for? 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.

Kali Linux: a complete pentesting toolkit facilitating smooth backtracking for working hackers About This Book Conduct network testing, surveillance, pen testing and forensics on MS Windows using Kali Linux Footprint, monitor, and audit your network and investigate any ongoing infestations Customize Kali Linux with this professional guide so it becomes your pen testing toolkit Who This Book Is For If you are a working ethical hacker who is looking to expand the offensive skillset with a thorough understanding of Kali Linux, then this is the book for you. Prior knowledge about Linux operating systems and the BASH terminal emulator along with Windows desktop and command line would be highly beneficial. What You Will Learn Set up Kali Linux for pen testing Map and enumerate your Windows network Exploit several common Windows network vulnerabilities Attack and defeat password schemes on Windows Debug and reverse-engineer Windows programs Recover lost files, investigate successful hacks and discover hidden data in innocent-looking files Catch and hold admin rights on the network, and maintain backdoors on the network after your initial testing is done In Detail Microsoft Windows is one of the two most common OS and managing its security has spawned the discipline of IT security. Kali Linux is the premier platform for testing and maintaining Windows security. Kali is built on the Debian distribution of Linux and shares the legendary stability of that OS. This lets you focus on using the network penetration, password cracking, forensics tools and not the OS. This book has the most advanced tools and techniques to reproduce the methods used by sophisticated hackers to make you an expert in Kali Linux penetration testing. First, you are introduced to Kali's top ten tools and other useful reporting tools. Then, you will find your way around your target network and determine known vulnerabilities to be able to exploit a system remotely.

Next, you will prove that the vulnerabilities you have found are real and exploitable. You will learn to use tools in seven categories of exploitation tools. Further, you perform web access exploits using tools like websploit and more. Security is only as strong as the weakest link in the chain. Passwords are often that weak link. Thus, you learn about password attacks that can be used in concert with other approaches to break into and own a network. Moreover, you come to terms with network sniffing, which helps you understand which users are using services you can exploit, and IP spoofing, which can be used to poison a system's DNS cache. Once you gain access to a machine or network, maintaining access is important. Thus, you not only learn penetrating in the machine you also learn Windows privilege's escalations. With easy to follow step-by-step instructions and support images, you will be able to quickly pen test your system and network. Style and approach This book is a hands-on guide for Kali Linux pen testing. This book will provide all the practical knowledge needed to test your network's security using a proven hacker's methodology. The book uses easy-to-understand yet professional language for explaining concepts.

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.

Hacking with Kali introduces you the most current distribution of the de facto standard tool for Linux pen testing. Starting with use of the Kali live CD and progressing through installation on hard drives, thumb

drives and SD cards, author James Broad walks you through creating a custom version of the Kali live distribution. You'll learn how to configure networking components, storage devices and system services such as DHCP and web services. Once you're familiar with the basic components of the software, you'll learn how to use Kali through the phases of the penetration testing lifecycle; one major tool from each phase is explained. The book culminates with a chapter on reporting that will provide examples of documents used prior to, during and after the pen test. This guide will benefit information security professionals of all levels, hackers, systems administrators, network administrators, and beginning and intermediate professional pen testers, as well as students majoring in information security. Provides detailed explanations of the complete penetration testing lifecycle Complete linkage of the Kali information, resources and distribution downloads Hands-on exercises reinforce topics

Over 80 recipes on how to identify, exploit, and test web application security with Kali Linux 2 About This Book Familiarize yourself with the most common web vulnerabilities a web application faces, and understand how attackers take advantage of them Set up a penetration testing lab to conduct a preliminary assessment of attack surfaces and run exploits Learn how to prevent vulnerabilities in web applications before an attacker can make the most of it Who This Book Is For This book 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. You should know the basics of operating a Linux environment and have some exposure to security technologies and tools. What You Will Learn Set up a penetration testing laboratory in a secure way Find out what information is useful to gather when performing penetration tests and where to look for it Use crawlers and spiders to investigate an entire website in minutes Discover security vulnerabilities in web applications in the web browser and using command-line tools Improve your testing efficiency with the use of automated vulnerability scanners Exploit vulnerabilities that require a complex setup, run custom-made exploits, and prepare for extraordinary scenarios Set up Man in the Middle attacks and use them to identify and exploit security flaws within the communication between users and the web server Create a malicious site that will find and exploit vulnerabilities in the user's web browser Repair the most common web vulnerabilities and understand how to prevent them becoming a threat to a site's security In Detail 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 and operating system that provides a huge array of testing tools, many of which can be used specifically to execute web penetration testing. This book will teach you, in the form step-by-step recipes, how to detect a wide array of vulnerabilities, exploit them to analyze their consequences, and ultimately buffer attackable surfaces so applications are more secure, for

you and your users. Starting from the setup of a testing laboratory, this book will give you the skills you need to cover every stage of a penetration test: from gathering information about the system and the application to identifying vulnerabilities through manual testing and the use of vulnerability scanners to both basic and advanced exploitation techniques that may lead to a full system compromise. Finally, we will put this into the context of 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 the book, you will have the required skills to identify, exploit, and prevent web application vulnerabilities. Style and approach Taking a recipe-based approach to web security, this book has been designed to cover each stage of a penetration test, with descriptions on how tools work and why certain programming or configuration practices can become security vulnerabilities that may put a whole system, or network, at risk. Each topic is presented as a sequence of tasks and contains a proper explanation of why each task is performed and what it accomplishes.

Discover Kali Linux And Take Your First Step Towards Becoming An Ethical Hacker! Are you a tech enthusiast who's curious about how computers and networks function? Are you looking for a new exciting career? Do you want an epic-sounding job title? Then ethical hacking is right for you. An ethical hacker (also known as a white hat hacker) is a cybersecurity expert who helps companies find and fix vulnerabilities in their software, networks, or websites. Some companies are ready to

pay tens of thousands of dollars for a single vulnerability! But how do you become an ethical hacker? You don't need a degree in IT or engineering to start hacking. It's one of those fields where experience matters much more than any formal qualifications you might have. All you need to start learning ethical hacking is a PC with the necessary tools installed. With this book, you'll get ready to start. This book will guide you through installing and using Kali Linux, an operating system designed specifically for the needs of ethical hackers. Here's what you'll learn: The top reasons why you should choose Linux as your operating system How to install Linux without technical knowledge Why Kali Linux is the best operating system for ethical hackers The best beginner-friendly hacking tools in Kali Linux The key principles of cybersecurity that every Internet user should know And much more! Unlike many other Linux books that are written with tech professionals in mind, this book is specifically aimed at beginners. This is why you'll find so many step-by-step guides and explanatory screenshots in the book. Just follow the instructions and enjoy your first successes! Get a taste of hacking with this beginner-friendly guide. Scroll up, click on "Buy Now with 1-Click", and Get Your Copy Now! Identify tools and techniques to secure and perform a penetration test on an AWS infrastructure using Kali Linux Key Features Efficiently perform penetration testing techniques on your public cloud instances Learn not only to cover loopholes but also to automate security monitoring and alerting within your cloud-based deployment pipelines A step-by-step guide that will help

you leverage the most widely used security platform to secure your AWS Cloud environment Book Description The cloud is taking over the IT industry. Any organization housing a large amount of data or a large infrastructure has started moving cloud-ward — and AWS rules the roost when it comes to cloud service providers, with its closest competitor having less than half of its market share. This highlights the importance of security on the cloud, especially on AWS. While a lot has been said (and written) about how cloud environments can be secured, performing external security assessments in the form of pentests on AWS is still seen as a dark art. This book aims to help pentesters as well as seasoned system administrators with a hands-on approach to pentesting the various cloud services provided by Amazon through AWS using Kali Linux. To make things easier for novice pentesters, the book focuses on building a practice lab and refining penetration testing with Kali Linux on the cloud. This is helpful not only for beginners but also for pentesters who want to set up a pentesting environment in their private cloud, using Kali Linux to perform a white-box assessment of their own cloud resources. Besides this, there is a lot of in-depth coverage of the large variety of AWS services that are often overlooked during a pentest — from serverless infrastructure to automated deployment pipelines. By the end of this book, you will be able to identify possible vulnerable areas efficiently and secure your AWS cloud environment. What you will learn Familiarize yourself with and pentest the most common external-facing AWS services Audit your own infrastructure and identify flaws, weaknesses, and

loopholes Demonstrate the process of lateral and vertical movement through a partially compromised AWS account Maintain stealth and persistence within a compromised AWS account Master a hands-on approach to pentesting Discover a number of automated tools to ease the process of continuously assessing and improving the security stance of an AWS infrastructure Who this book is for If you are a security analyst or a penetration tester and are interested in exploiting Cloud environments to reveal vulnerable areas and secure them, then this book is for you. A basic understanding of penetration testing, cloud computing, and its security concepts is mandatory.

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 property, you will fail in getting access to this awesome software, and you will be irritated. But just like existing problems, there is also a wide range of troubleshooters which you can learn through this book, helping you get rid of all forms of problems that come in the way of installation. This book is the fourth part of this series. It is a beginner's guide to cover all the essential topics related to the Linux Operating System. You will discover: -What is Linux -History and Benefits of Linux -Ubuntu Basics and Installing Linux -Managing Software and Hardware -The Command-Line Terminal -Useful Applications -Security Protocols -Scripting, I/O

Redirection, Managing Directories -And a WHOLE lot more!

Kali Linux is an open source Linux distribution for security, digital forensics, and penetration testing tools, and is now an operating system for Linux users. It is the successor to BackTrack, the world's most popular penetration testing distribution tool. In this age, where online information is at its most vulnerable, knowing how to execute penetration testing techniques such as wireless and password attacks, which hackers use to break into your system or network, help you plug loopholes before it's too late and can save you countless hours and money.Kali Linux Cookbook, Second Edition is an invaluable guide, teaching you how to install Kali Linux and set up a virtual environment to perform your tests. You will learn how to eavesdrop and intercept traffic on wireless networks, bypass intrusion detection systems, attack web applications, check for open ports, and perform data forensics.This book follows the logical approach of a penetration test from start to finish with many screenshots and illustrations that help to explain each tool in detail. This book serves as an excellent source of information for security professionals and novices alike.

Kali Linux Network Scanning Cookbook is intended for information security professionals and casual security enthusiasts alike. It will provide the foundational principles for the novice reader but will also introduce scripting techniques and in-depth analysis for the more advanced audience. Whether you are brand new to Kali Linux or a seasoned veteran, this book will aid in both

understanding and ultimately mastering many of the most powerful and useful scanning techniques in the industry. It is assumed that the reader has some basic security testing experience.

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!

If you are a security professional, pentester, or anyone interested in getting to grips with wireless penetration testing, this is the book for you. Some familiarity with Kali Linux and wireless concepts is beneficial.

? Are you interested in learning more about hacking and how you can use these techniques to keep yourself and your network as safe as possible? ? Would you like to work with Kali Linux to protect your network and to make sure that hackers are not able to get onto your computer and cause trouble or steal your personal information? ? Have you ever been interested in learning more about the process of

hacking, how to avoid being taken advantage of, and how you can use some of techniques for your own needs? This guidebook is going to provide us with all of the information that we need to know about Hacking with Linux. Many people worry that hacking is a bad process and that it is not the right option for them. The good news here is that hacking can work well for not only taking information and harming others but also for helping you keep your own network and personal information as safe as possible. Inside this guidebook, we are going to take some time to explore the world of hacking, and why the Kali Linux system is one of the best to help you get this done. We explore the different types of hacking, and why it is beneficial to learn some of the techniques that are needed to perform your own hacks and to see the results that we want with our own networks. In this guidebook, we will take a look at a lot of the different topics and techniques that we need to know when it comes to working with hacking on the Linux system. Some of the topics that we are going to take a look at here include: The different types of hackers that we may encounter and how they are similar and different. How to install the Kali Linux onto your operating system to get started. The basics of cybersecurity, web security, and cyberattacks and how these can affect your computer system and how a hacker will try to use you. The different types of malware that hackers can

use against you. How a man in the middle, DoS, Trojans, viruses, and phishing can all be tools of the hacker. And so much more. Hacking is often an option that most people will not consider because they worry that it is going to be evil, or that it is only used to harm others. But as we will discuss in this guidebook, there is so much more to the process than this.

Kali Linux RevealedMastering the Penetration Testing Distribution

This book is a fully focused, structured book providing guidance on developing practical penetration testing skills by demonstrating cutting-edge hacker tools and techniques. It offers you all of the essential lab preparation and testing procedures that reflect real-world attack scenarios from a business perspective, in today's digital age.

Do you want to learn about how to hack using Kali Linux within a short time span? Do you want to learn about how to perform an actual attack and become a professional hacker? Besides focusing on the introduction to Kali Linux, there is a chapter where by we have discussed more about the Kali Linux installation. You can install Kali Linux in different ways. For instance, you can install the Kali Linux operating system to run as the primary operating system. It is also possible to install Kali Linux so that it may run on the "Live mode".When using Kali Linux, you can also customize the operating system.

Each of the tools present in the Kali Linux operating system comes in handy when handling different tasks. There is the chapter where we have discussed about how to carry out a reconnaissance. There are two types of reconnaissance; passive and active. While reading through the Hacking with Kali Linux handbook, you can learn more about the types of reconnaissance. As an attacker or penetration tester, the reconnaissance will come in handy when gathering information before you can launch an attack. The pilot study makes sure that you will gain access to some important pieces of information that will ensure that the attack can progress in a flawless manner. As a penetration tester or an attacker, you should make sure that you have assessed the situation accordingly. Also, you must make sure that you have chosen a suitable target first. When using Kali Linux, you should make sure that you have not installed external applications. Some of the tools provided by Kali Linux make sure that you can gain access to administrator passwords as well as usernames. You can then go ahead to use this information to gain access to the network or target's server. Although you may possess little knowledge about how to hack using Kali Linux, this handbook will guide you accordingly. In this book, you will learn about: The Kali Linux installation. How to customize Kali Linux. Examples on how to hack using Kali Linux. How to plan an attack. How to launch an

attack. The tools offered by Kali Linux. And more... You may just be a beginner who also possesses a limited amount of knowledge about hacking; the only limitation to becoming a professional hacker is yourself. Would you like to know more?Scroll to the top of the page and select the BUY NOW button! 55% off for bookstores! Paperback CLR Only for a Limited Time Discounted Retail Price at $49.99 Instead of $57.99 Buy it right now and let your customers be thankful to you for this book! Your ultimate guide to pentesting with Kali Linux Kali is a popular and powerful Linux distribution used by cybersecurity professionals around the world. Penetration testers must master Kali's varied library of tools to be effective at their work. The Kali Linux Penetration Testing Bible is the hands-on and methodology guide for pentesting with Kali. You'll discover everything you need to know about the tools and techniques hackers use to gain access to systems like yours so you can erect reliable defenses for your virtual assets. Whether you're new to the field or an established pentester, you'll find what you need in this comprehensive guide. Build a modern dockerized environment Discover the fundamentals of the bash language in Linux Use a variety of effective techniques to find vulnerabilities (OSINT, Network Scan, and more) Analyze your findings and identify false positives and uncover advanced subjects, like buffer overflow, lateral

movement, and privilege escalation Apply practical and efficient pentesting workflows Learn about Modern Web Application Security Secure SDLC Automate your penetration testing with Python The contents in this book will provide practical hands on implementation and demonstration guide on how you can use Kali Linux to deploy various attacks on both wired and wireless networks. If you are truly interested in becoming an Ethical Hacker or Penetration Tester, this book is for you.NOTE: If you attempt to use any of this tools on a wired or wireless network without being authorized and you disturb or damage any systems, that would be considered illegal black hat hacking. Therefore, I would like to encourage all readers to implement any tool described in this book for WHITE HAT USE ONLY!BUY THIS BOOK NOW AND GET STARTED TODAY!This book will cover: -How to Install Virtual Box & Kali Linux-Pen Testing @ Stage 1, Stage 2 and Stage 3-What Penetration Testing Standards exist-How to scan for open ports, host and network devices-Burp Suite Proxy setup and Spidering hosts-How to deploy SQL Injection with SQLmap-How to implement Dictionary Attack with Airodump-ng-How to deploy ARP Poisoning with EtterCAP-How to capture Traffic with Port Mirroring & with Xplico-How to deploy Passive Reconnaissance-How to implement MITM Attack with Ettercap & SSLstrip-How to Manipulate Packets with Scapy-How to

deploy Deauthentication Attack-How to capture IPv6 Packets with Parasite6-How to deploy Evil Twin Deauthentication Attack with mdk3-How to deploy DoS Attack with MKD3-How to implement Brute Force Attack with TCP Hydra-How to deploy Armitage Hail Mary-The Metasploit Framework-How to use SET aka Social-Engineering Toolkit and more.BUY THIS BOOK NOW AND GET STARTED TODAY!

Copyright: b8b60bdce8a621ab4bd5061bfa604005