kali linux hacking pdf

kali linux hacking pdf is a search query that unlocks a vast world of digital security knowledge for aspiring ethical hackers and cybersecurity professionals. This article aims to be your definitive guide to understanding what a Kali Linux hacking PDF entails, why it's a valuable resource, and how to leverage it effectively. We will explore the core functionalities of Kali Linux, delve into the types of hacking techniques often covered in such documents, discuss the ethical considerations surrounding their use, and guide you on finding reliable and legal PDF resources. Whether you're a beginner looking to understand the fundamentals of penetration testing or an experienced professional seeking to expand your skillset, this comprehensive overview will equip you with the knowledge to navigate the landscape of Kali Linux hacking PDFs.

Understanding Kali Linux for Hacking

Kali Linux is a Debian-based Linux distribution designed for digital forensics and penetration testing. It comes pre-installed with hundreds of tools that cater to various security tasks, from network scanning and vulnerability analysis to web application testing and password cracking. Its open-source nature and the continuous development by Offensive Security have made it a de facto standard in the cybersecurity community. For anyone interested in cybersecurity, understanding Kali Linux is a fundamental step, and a Kali Linux hacking PDF often serves as an excellent starting point for this exploration.

The Core Purpose of Kali Linux

The primary purpose of Kali Linux is to provide security professionals with a robust and comprehensive environment for conducting security assessments. It is not designed for general-purpose computing but rather for specialized tasks. Its strength lies in its curated collection of tools, meticulously selected to cover the entire spectrum of penetration testing methodologies. This focus ensures that users have access to the most effective and up-to-date instruments for identifying and exploiting vulnerabilities in systems and networks.

Key Features and Benefits of Kali Linux

Kali Linux boasts several key features that make it indispensable for hacking and security auditing. These include its extensive repository of security tools, its customizable nature, and its live boot capability, which allows users to run it directly from a USB drive or DVD without installation. The distribution is also known for its strong community support, ensuring that users can find help and resources readily available. For those new to the

platform, a Kali Linux hacking PDF can demystify these features and showcase their practical applications.

- Extensive collection of pre-installed security tools.
- Live boot functionality for portable security assessments.
- Customizable environment to suit specific needs.
- Regular updates and security patches.
- Active community support and extensive documentation.

What to Expect in a Kali Linux Hacking PDF

A Kali Linux hacking PDF typically serves as a guide or tutorial for utilizing the distribution and its associated tools for various cybersecurity tasks. These documents can range from beginner-friendly introductions to advanced deep dives into specific penetration testing methodologies. Understanding the content of these PDFs is crucial to ensure they align with your learning objectives and ethical boundaries.

Common Topics Covered in Kali Linux Hacking PDFs

The topics found within a Kali Linux hacking PDF are diverse and cover a wide array of security domains. Beginners might find guides on setting up Kali Linux, navigating the operating system, and understanding basic networking concepts. More advanced PDFs will delve into specific attack vectors, exploitation techniques, and defensive strategies. Regardless of the level, these documents often aim to provide practical, hands-on knowledge.

Some of the most frequently encountered topics include:

- Introduction to penetration testing methodologies.
- Installation and configuration of Kali Linux.
- Network reconnaissance and information gathering.
- Vulnerability scanning and analysis.
- Exploitation techniques for various services.
- Web application security testing.
- Password cracking and brute-force attacks.

- Wireless network security assessment.
- Forensic analysis using Kali Linux tools.

Essential Tools Explained in PDFs

Kali Linux comes equipped with a vast arsenal of tools, and any comprehensive Kali Linux hacking PDF will likely highlight some of the most crucial ones. These tools are the backbone of penetration testing, enabling attackers (ethical or otherwise) to probe systems for weaknesses. Learning how to use these tools effectively is a primary goal for anyone studying these documents.

Key tools often discussed include:

1. **Nmap:** A powerful network scanner used for host discovery and service enumeration.
2. **Metasploit Framework:** A widely used platform for developing and executing exploit code.
3. **Wireshark:** A network protocol analyzer used to capture and inspect network traffic.
4. **Aircrack-ng:** A suite of tools for assessing wireless network security.
5. **Burp Suite:** An integrated platform for performing security testing of web applications.
6. **John the Ripper:** A popular password cracking tool.

Ethical Hacking and Legal Considerations

It is paramount to emphasize that any knowledge gained from a Kali Linux hacking PDF must be used ethically and legally. Penetration testing and security auditing are legitimate practices when performed with explicit permission from the system owner. Unauthorized access to computer systems is a serious crime with severe consequences.

The Importance of Ethical Hacking

Ethical hacking, also known as penetration testing or white-hat hacking, involves using hacking techniques to identify vulnerabilities in systems, networks, and applications with the permission of their owners. The goal is

to improve security by proactively addressing these weaknesses before malicious actors can exploit them. A Kali Linux hacking PDF should always be approached with this ethical framework in mind.

Legal Ramifications of Unauthorized Access

Engaging in any hacking activity without proper authorization can lead to severe legal penalties, including substantial fines and imprisonment. Laws such as the Computer Fraud and Abuse Act (CFAA) in the United States and similar legislation worldwide criminalize unauthorized access to computer systems. Therefore, when studying Kali Linux hacking PDFs, it is essential to practice only in controlled, legal environments, such as virtual labs or authorized testing scenarios.

Finding and Utilizing Kali Linux Hacking PDFs

Locating reliable and relevant Kali Linux hacking PDF resources is the next step for those looking to learn. However, it's crucial to approach this search with caution to avoid malware and to ensure the legality of the content.

Sources for Legitimate Kali Linux Hacking Resources

Many reputable sources offer educational materials related to Kali Linux and ethical hacking. The official Kali Linux website often provides documentation and links to training materials. Cybersecurity training platforms, online learning websites, and reputable tech publishers are also excellent places to find high-quality PDFs and other resources. Always prioritize official documentation and well-regarded educational providers.

How to Effectively Learn from Kali Linux Hacking PDFs

Simply reading a Kali Linux hacking PDF is rarely enough to gain practical proficiency. Effective learning involves a combination of theoretical understanding and hands-on practice. Setting up a virtual lab environment using tools like VirtualBox or VMware is essential for safely experimenting with Kali Linux and its tools. Follow along with the exercises, experiment with different parameters, and try to understand the underlying principles of each technique. Consistent practice and a commitment to continuous learning are key to mastering the skills outlined in these invaluable resources.

Frequently Asked Questions

Where can I find reliable and up-to-date Kali Linux hacking PDF guides for beginners?

For reliable and up-to-date Kali Linux hacking PDF guides, start with official Kali Linux documentation and resources. Many security professionals and educational platforms also offer free or paid PDFs. Look for resources published within the last year to ensure relevance, as Kali Linux and its tools are frequently updated. Websites like Offensive Security's official blog, Cybrary, or dedicated cybersecurity forums often have curated lists of recommended resources.

Are there ethical hacking PDFs for Kali Linux that cover penetration testing methodologies?

Yes, many Kali Linux hacking PDFs specifically focus on ethical hacking and penetration testing methodologies. These guides typically cover the phases of a penetration test, including reconnaissance, scanning, vulnerability analysis, exploitation, post-exploitation, and reporting. They will also detail the use of various Kali Linux tools for each phase, such as Nmap, Metasploit, Burp Suite, and Wireshark.

What are some popular topics covered in Kali Linux hacking PDFs for advanced users?

Advanced Kali Linux hacking PDFs often delve into more specialized areas. Popular topics include web application penetration testing (SQL injection, XSS, CSRF), network security assessments, wireless network attacks, social engineering techniques, malware analysis, exploit development, cryptography, and cloud security. These guides assume a foundational understanding of Kali Linux and its core tools.

Is it legal to download and use Kali Linux hacking PDFs for learning purposes?

Generally, it is legal to download and use Kali Linux hacking PDFs for learning purposes, provided they are obtained from legitimate sources and the content itself is educational. The legality hinges on your intent and actions. Using the knowledge gained from these PDFs to perform unauthorized access on computer systems is illegal and unethical. Always ensure you are practicing ethical hacking within legal boundaries, such as on your own systems or with explicit permission.

What are the key benefits of using Kali Linux PDFs

to learn hacking?

The key benefits of using Kali Linux PDFs to learn hacking include structured learning paths, access to comprehensive tool explanations, practical examples and case studies, and self-paced learning opportunities. Kali Linux is a purpose-built distribution for penetration testing, and PDFs dedicated to it often provide concise, hands-on guidance that complements theoretical knowledge, making complex concepts more accessible and actionable.

Additional Resources

Here are 9 book titles related to Kali Linux hacking, presented in a numbered list with descriptions:

1. *Kali Linux Revealed: Mastering the Penetration Testing Distribution*
This comprehensive guide is an official training manual from Offensive Security, the creators of Kali Linux. It delves deep into the core functionalities and architecture of Kali, teaching readers how to effectively install, configure, and utilize its vast array of tools for penetration testing and ethical hacking. The book covers everything from basic system administration to advanced exploitation techniques, making it an indispensable resource for serious Kali users.

2. *The Hacker Playbook 3: Practical Guide To Penetration Testing With Kali Linux*
Designed as a practical, hands-on guide, this book walks users through realistic penetration testing scenarios. It emphasizes building a lab environment and using Kali Linux tools in a systematic approach to compromise systems. The content focuses on actionable advice and methodologies that can be immediately applied to real-world security assessments.

3. *Penetration Testing: A Hands-On Introduction to Hacking*
While not exclusively focused on Kali Linux, this book heavily features its use as the primary platform for conducting penetration tests. It provides a foundational understanding of hacking concepts, explaining how to use various Kali tools for reconnaissance, scanning, exploitation, and post-exploitation phases. The book bridges theoretical knowledge with practical application, making it accessible to beginners.

4. *Mastering Kali Linux for Advanced Penetration Testing*
This title targets intermediate to advanced users who want to go beyond the basics of Kali Linux. It explores sophisticated techniques and tools within Kali, focusing on advanced exploitation, bypassing security measures, and covering specialized areas like wireless and web application penetration testing. The book aims to equip readers with the skills to tackle complex security challenges.

5. *Penetration Testing with Kali Linux - Second Edition*
This book offers a structured approach to learning penetration testing methodologies using Kali Linux. It covers the entire penetration testing

lifecycle, from planning and reconnaissance to reporting, with a strong emphasis on practical exercises and real-world examples. Readers will learn how to leverage Kali's robust toolkit to identify vulnerabilities and demonstrate their impact.

6. *BackBox Linux & Kali Linux - Your Essential Guide To Penetration Testing & Security Auditing*
This comparative guide highlights the strengths of both BackBox and Kali Linux for security professionals. It focuses on using these distributions to perform comprehensive penetration tests and security audits. The book explains how to effectively utilize the bundled tools for various security assessments and to discover potential weaknesses in systems.

7. *Penetration Testing Essentials: Foundational Knowledge for Ethical Hacking*
This book provides the fundamental concepts and techniques necessary for ethical hacking, with Kali Linux serving as the primary operating system and toolkit. It covers essential topics such as network scanning, vulnerability analysis, and basic exploit development. The aim is to build a solid understanding of the ethical hacking process before delving into more advanced practices.

8. *Certified Ethical Hacker (CEH) v11 Study Guide*
While not exclusively about Kali Linux, this study guide for the Certified Ethical Hacker certification heavily utilizes Kali Linux as the platform for demonstrating the required skills. It covers the broad spectrum of ethical hacking domains, including information gathering, vulnerability assessment, and intrusion detection, all often practiced and demonstrated using Kali's tools. This book is ideal for those seeking formal certification in ethical hacking.

9. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*
This introductory book demystifies the world of hacking for beginners, with Kali Linux being a central component of the practical examples. It breaks down complex concepts into easily digestible lessons, explaining the fundamentals of reconnaissance, scanning, and exploitation using readily available tools. The book aims to provide a clear and accessible entry point into ethical hacking using Kali.

Kali Linux Hacking Pdf

Kali Linux Hacking PDF: A Comprehensive Guide to Ethical Hacking and Penetration Testing

Ebook Title: Kali Linux: The Ethical Hacker's Handbook

Outline:

Introduction: What is Kali Linux? Why use it for ethical hacking? Setting up a virtual machine (VM) for safe practice.
Chapter 1: Fundamental Linux Commands: Essential commands for navigating, managing files, and using the terminal.
Chapter 2: Network Scanning and Enumeration: Tools for identifying network devices, services, and vulnerabilities. (Nmap, Nessus)
Chapter 3: Vulnerability Assessment: Identifying weaknesses in systems and applications. (Metasploit, OWASP ZAP)
Chapter 4: Penetration Testing Methodologies: Understanding different penetration testing approaches (e.g., black box, white box).
Chapter 5: Social Engineering and Phishing: Exploring the human element in security breaches and ethical considerations.
Chapter 6: Wireless Network Security: Assessing and securing wireless networks (Aircrack-ng).
Chapter 7: Web Application Security: Testing web application vulnerabilities (Burp Suite, SQLmap).
Chapter 8: Report Writing and Ethical Considerations: Documenting findings and adhering to ethical guidelines.
Conclusion: Recap and future learning resources.

Kali Linux: The Ethical Hacker's Handbook – A Deep Dive

This comprehensive guide explores the powerful capabilities of Kali Linux, a leading operating system for ethical hacking and penetration testing. This article delves into each section of the ebook, providing a detailed understanding of the topics covered. Remember, all activities described here should be performed only with explicit permission from the system owner. Unauthorized access is illegal and unethical.

Introduction: Getting Started with Kali Linux

Kali Linux is a Debian-based Linux distribution specifically designed for penetration testing and digital forensics. Its popularity stems from its extensive collection of pre-installed security tools, making it a go-to resource for security professionals and aspiring ethical hackers. This introductory chapter provides a foundational understanding of what Kali Linux is and why it's crucial in the cybersecurity landscape. We'll cover the ethical implications of using such powerful tools, emphasizing the importance of responsible usage and legal compliance.

The guide also offers detailed instructions on setting up Kali Linux within a virtual machine (VM).

Using a VM is crucial; it provides a safe and isolated environment to experiment with hacking tools without risking your main operating system. Popular VM software like VirtualBox or VMware will be discussed, along with step-by-step setup instructions and recommended configurations to ensure optimal performance and security.

Chapter 1: Mastering Fundamental Linux Commands

Before diving into advanced penetration testing tools, a solid understanding of fundamental Linux commands is essential. This chapter serves as a crash course in navigating the Linux terminal. We'll cover core commands such as `ls`, `cd`, `pwd`, `mkdir`, `rm`, `cp`, `mv`, `grep`, and `find`. Understanding these commands enables efficient file management, navigation through directories, and effective interaction with Kali Linux's tools. This chapter will be practical, focusing on examples and real-world applications relevant to penetration testing.

Chapter 2: Network Scanning and Enumeration – Unveiling Network Vulnerabilities

Network scanning and enumeration are critical initial steps in any penetration test. This chapter introduces essential tools like Nmap and Nessus. Nmap (Network Mapper) is a powerful and versatile network scanner used to discover hosts and services on a network, identify open ports, and detect operating systems. We'll cover different Nmap scan types, including SYN scans, UDP scans, and version detection. The chapter will also explore how to interpret Nmap output to identify potential vulnerabilities.

Nessus, a commercial vulnerability scanner (though a free version exists), complements Nmap by providing detailed information about identified vulnerabilities. We'll demonstrate how to use Nessus to perform vulnerability scans and analyze the results to prioritize potential threats. The chapter concludes by comparing and contrasting Nmap and Nessus, highlighting their strengths and limitations.

Chapter 3: Vulnerability Assessment – Identifying System Weaknesses

This chapter focuses on identifying specific vulnerabilities within systems and applications. We'll delve into the use of Metasploit, a widely-used penetration testing framework. Metasploit provides a vast library of exploits, allowing ethical hackers to test the resilience of systems against known vulnerabilities. This chapter will cover the basics of Metasploit, demonstrating how to use it to find and exploit vulnerabilities, along with the ethical considerations and importance of responsible disclosure.

OWASP ZAP (Zed Attack Proxy) is another essential tool for web application security testing. We will cover techniques to use ZAP for identifying common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). The chapter emphasizes the importance of understanding the underlying vulnerabilities rather than simply relying on automated tools.

Chapter 4: Penetration Testing Methodologies – Strategic Approaches to Security Assessment

This chapter delves into the strategic aspects of penetration testing. We will explore various methodologies, including black box testing (no prior knowledge of the system), white box testing (full system knowledge), and grey box testing (partial system knowledge). Each methodology has its advantages and disadvantages; understanding these nuances allows for a more targeted and effective approach. We will discuss the planning phase, execution phase, and reporting phase of a penetration test, highlighting the importance of documentation and responsible disclosure.

Chapter 5: Social Engineering and Phishing – Exploiting the Human Factor

Social engineering exploits human psychology to gain unauthorized access to systems or information. This chapter covers various social engineering techniques, including phishing, baiting, and pretexting. We'll explore the ethical implications of social engineering and emphasize the importance of responsible and legal usage. The chapter will also discuss techniques for defending against social engineering attacks.

Chapter 6: Wireless Network Security – Securing the Airwaves

Wireless networks are often vulnerable to attacks. This chapter introduces Aircrack-ng, a suite of tools for assessing the security of wireless networks. We'll cover techniques for performing Wi-Fi network scans, identifying vulnerable networks, and cracking WEP and WPA/WPA2 passwords. Ethical considerations surrounding wireless network penetration testing are also discussed.

Chapter 7: Web Application Security – Protecting Against Online Threats

Web applications are frequently targeted by attackers. This chapter explores the vulnerabilities of web applications and demonstrates techniques for testing their security. We'll utilize Burp Suite, a widely-used web application security testing tool, to identify common vulnerabilities such as SQL injection, XSS, and CSRF. The chapter also covers SQLmap, a powerful tool specifically designed for detecting and exploiting SQL injection vulnerabilities.

Chapter 8: Report Writing and Ethical Considerations – Professionalism and Responsibility

This chapter emphasizes the critical role of thorough and accurate reporting in penetration testing. We will discuss the importance of clear and concise documentation, outlining the necessary components of a professional penetration testing report. We'll cover best practices for presenting findings, prioritizing vulnerabilities, and providing remediation recommendations. The chapter concludes by reiterating the paramount importance of adhering to ethical guidelines and legal regulations throughout the entire penetration testing process.

Conclusion: Continuing Your Journey in Ethical Hacking

This concluding chapter summarizes the key concepts covered in the ebook and provides resources for continued learning. We'll suggest further reading, online courses, and certifications to enhance your skills and knowledge in ethical hacking and penetration testing.

FAQs:

1. Is Kali Linux legal to use? Kali Linux itself is legal; however, using it for unauthorized access is illegal.
2. Do I need programming skills to use Kali Linux? Basic command-line skills are helpful, but not necessarily advanced programming.
3. Is it safe to use Kali Linux on my primary computer? It's strongly recommended to use a virtual machine.
4. What are the ethical implications of penetration testing? Always obtain explicit permission before testing any system.
5. What are the best resources for learning more about ethical hacking? Numerous online courses, certifications (e.g., CEH), and books are available.
6. How do I choose the right penetration testing methodology? This depends on the scope and objectives of the test and the information available.
7. What is the difference between Nmap and Nessus? Nmap scans for open ports and services, while Nessus identifies vulnerabilities.
8. How do I write a professional penetration testing report? A report should clearly outline the methodology, findings, and remediation recommendations.

9. Where can I find legal and ethical guidelines for penetration testing? Organizations like OWASP and SANS offer valuable resources.

Related Articles:

1. Nmap for Beginners: A Practical Guide: A step-by-step tutorial on using Nmap for network scanning.
2. Metasploit Framework: Exploiting Vulnerabilities Ethically: A guide to using Metasploit for penetration testing.
3. OWASP Top 10 Web Application Security Risks: An overview of the most common web application vulnerabilities.
4. Setting up a Virtual Machine for Penetration Testing: A detailed guide on creating a secure VM environment.
5. Introduction to Social Engineering Techniques: Exploring various social engineering tactics and defenses.
6. Wireless Network Security Fundamentals: Understanding wireless security protocols and vulnerabilities.
7. Ethical Hacking: A Career Path in Cybersecurity: A look at the career opportunities in ethical hacking.
8. Understanding Penetration Testing Methodologies: A deep dive into different penetration testing approaches.
9. Writing Effective Penetration Testing Reports: Best practices for creating professional and informative reports.

kali linux hacking pdf: Kali Linux - An Ethical Hacker's Cookbook Himanshu Sharma, 2017-10-17 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.

kali linux hacking pdf: Linux Basics for Hackers OccupyTheWeb, 2018-12-04 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?

kali linux hacking pdf: *Beginning Ethical Hacking with Kali Linux* Sanjib Sinha, 2018-11-29 Get started in white-hat ethical hacking using Kali Linux. This book starts off by giving you an overview of security trends, where you will learn the OSI security architecture. This will form the foundation for the rest of Beginning Ethical Hacking with Kali Linux. With the theory out of the way, you'll move on to an introduction to VirtualBox, networking, and common Linux commands, followed by the step-by-step procedure to build your own web server and acquire the skill to be anonymous . When you have finished the examples in the first part of your book, you will have all you need to carry out safe and ethical hacking experiments. After an introduction to Kali Linux, you will carry out your first penetration tests with Python and code raw binary packets for use in those tests. You will learn how to find secret directories on a target system, use a TCP client in Python, and scan ports using NMAP. Along the way you will discover effective ways to collect important information, track email, and use important tools such as DMITRY and Maltego, as well as take a look at the five phases of penetration testing. The coverage of vulnerability analysis includes sniffing and spoofing, why ARP poisoning is a threat, how SniffJoke prevents poisoning, how to analyze protocols with Wireshark, and using sniffing packets with Scapy. The next part of the book shows you detecting SQL injection vulnerabilities, using sqlmap, and applying brute force or password attacks. Besides learning these tools, you will see how to use OpenVas, Nikto, Vega, and Burp Suite. The book will explain the information assurance model and the hacking framework Metasploit, taking you through important commands, exploit and payload basics. Moving on to hashes and passwords you will learn password testing and hacking techniques with John the Ripper and Rainbow. You will then dive into classic and modern encryption techniques where you will learn the conventional cryptosystem. In the final chapter you will acquire the skill of exploiting remote Windows and Linux systems and you will learn how to own a target completely. What You Will LearnMaster common Linux commands and networking techniques Build your own Kali web server and learn to be anonymous Carry out penetration testing using Python Detect sniffing attacks and SQL injection vulnerabilities Learn tools such as SniffJoke, Wireshark, Scapy, sqlmap, OpenVas, Nikto, and Burp Suite Use Metasploit with Kali Linux Exploit remote Windows and Linux systemsWho This Book Is For Developers new to ethical hacking with a basic understanding of Linux programming.

kali linux hacking pdf: 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 KaliÃ¢??s expansive security capabilities and helps you identify the tools you need to conduct a wide range of security tests and penetration tests. YouÃ¢??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. YouÃ¢??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 whatÃ¢??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

kali linux hacking pdf: Network Scanning Cookbook Sairam Jetty, 2018-09-29 Discover network vulnerabilities and threats to design effective network security strategies Key FeaturesPlunge into scanning techniques using the most popular toolsEffective vulnerability assessment techniques to safeguard network infrastructureExplore the Nmap Scripting Engine (NSE) and the features used for port and vulnerability scanningBook Description Network scanning is a discipline of network security that identifies active hosts on networks and determining whether there are any vulnerabilities that could be exploited. Nessus and Nmap are among the top tools that enable you to scan your network for vulnerabilities and open ports, which can be used as back doors into a network. Network Scanning Cookbook contains recipes for configuring these tools in your infrastructure that get you started with scanning ports, services, and devices in your network. As you progress through the chapters, you will learn how to carry out various key scanning tasks, such as firewall detection, OS detection, and access management, and will look at problems related to vulnerability scanning and exploitation in the network. The book also contains recipes for assessing remote services and the security risks that they bring to a network infrastructure. By the end of the book, you will be familiar with industry-grade tools for network scanning, and techniques for vulnerability scanning and network protection. What you will learnInstall and configure Nmap and Nessus in your network infrastructurePerform host discovery to identify network devicesExplore best practices for vulnerability scanning and risk assessmentUnderstand network enumeration with Nessus and NmapCarry out configuration audit using Nessus for various platformsWrite custom Nessus and Nmap scripts on your ownWho this book is for If you’re a network engineer or information security professional wanting to protect your networks and perform advanced scanning and remediation for your network infrastructure, this book is for you.

kali linux hacking pdf: The Basics of Hacking and Penetration Testing Patrick Engebretson, 2013-06-24 The Basics of Hacking and Penetration Testing, Second Edition, serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. The book teaches students how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. It provides a simple and clean explanation of how to effectively utilize these tools, along with a four-step methodology for conducting a penetration test or hack, thus equipping students with the know-how required to jump start their careers and gain a better understanding of offensive security.Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. Tool coverage includes: Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. This is complemented by PowerPoint slides for use in class.This book is an ideal resource for security consultants, beginning InfoSec professionals, and students. - Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases - Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University - Utilizes the Kali Linux distribution and focuses on the seminal tools required to complete a penetration test

kali linux hacking pdf: Hacking with Kali James Broad, Andrew Bindner, 2013-12-05 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

kali linux hacking pdf: Penetration Testing Georgia Weidman, 2014-06-14 Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own Metasploit modules –Automate social-engineering attacks –Bypass antivirus software –Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.

kali linux hacking pdf: Kali Linux Wireless Penetration Testing Cookbook Sean-Philip Oriyano, 2017-12-13 Over 60 powerful recipes to scan, exploit, and crack wireless networks for ethical purposes About This Book Expose wireless security threats through the eyes of an attacker, Recipes to help you proactively identify vulnerabilities and apply intelligent remediation, Acquire and apply key wireless pentesting skills used by industry experts Who This Book Is For If you are a security professional, administrator, and a network professional who wants to enhance their wireless penetration testing skills and knowledge then this book is for you. Some prior experience with networking security and concepts is expected. What You Will Learn Deploy and configure a wireless cyber lab that resembles an enterprise production environment Install Kali Linux 2017.3 on your laptop and configure the wireless adapter Learn the fundamentals of commonly used wireless penetration testing techniques Scan and enumerate Wireless LANs and access points Use vulnerability scanning techniques to reveal flaws and weaknesses Attack Access Points to gain access to critical networks In Detail More and more organizations are moving towards wireless networks, and Wi-Fi is a popular choice. The security of wireless networks is more important than ever before due to the widespread usage of Wi-Fi networks. This book contains recipes that will enable you to maximize the success of your wireless network testing using the advanced ethical hacking features of Kali Linux. This book will go through techniques associated with a wide range of wireless penetration tasks, including WLAN discovery scanning, WEP cracking, WPA/WPA2 cracking, attacking access point systems, operating system identification, vulnerability mapping, and validation of results. You will learn how to utilize the arsenal of tools available in Kali Linux to penetrate any wireless networking environment. You will also be shown how to identify remote services, how to assess security risks, and how various attacks are performed. By finishing the

recipes, you will feel confident conducting wireless penetration tests and will be able to protect yourself or your organization from wireless security threats. Style and approach The book will provide the foundation principles, techniques, and in-depth analysis to effectively master wireless penetration testing. It will aid you in understanding and mastering many of the most powerful and useful wireless testing techniques in the industry.

kali linux hacking pdf: The Ultimate Kali Linux Book Glen D. Singh, 2022-02-24 The most comprehensive guide to ethical hacking and penetration testing with Kali Linux, from beginner to professional Key Features Learn to compromise enterprise networks with Kali Linux Gain comprehensive insights into security concepts using advanced real-life hacker techniques Use Kali Linux in the same way ethical hackers and penetration testers do to gain control of your environment Purchase of the print or Kindle book includes a free eBook in the PDF format Book DescriptionKali Linux is the most popular and advanced penetration testing Linux distribution within the cybersecurity industry. Using Kali Linux, a cybersecurity professional will be able to discover and exploit various vulnerabilities and perform advanced penetration testing on both enterprise wired and wireless networks. This book is a comprehensive guide for those who are new to Kali Linux and penetration testing that will have you up to speed in no time. Using real-world scenarios, you'll understand how to set up a lab and explore core penetration testing concepts. Throughout this book, you'll focus on information gathering and even discover different vulnerability assessment tools bundled in Kali Linux. You'll learn to discover target systems on a network, identify security flaws on devices, exploit security weaknesses and gain access to networks, set up Command and Control (C2) operations, and perform web application penetration testing. In this updated second edition, you'll be able to compromise Active Directory and exploit enterprise networks. Finally, this book covers best practices for performing complex web penetration testing techniques in a highly secured environment. By the end of this Kali Linux book, you'll have gained the skills to perform advanced penetration testing on enterprise networks using Kali Linux.What you will learn Explore the fundamentals of ethical hacking Understand how to install and configure Kali Linux Perform asset and network discovery techniques Focus on how to perform vulnerability assessments Exploit the trust in Active Directory domain services Perform advanced exploitation with Command and Control (C2) techniques Implement advanced wireless hacking techniques Become well-versed with exploiting vulnerable web applications Who this book is for This pentesting book is for students, trainers, cybersecurity professionals, cyber enthusiasts, network security professionals, ethical hackers, penetration testers, and security engineers. If you do not have any prior knowledge and are looking to become an expert in penetration testing using the Kali Linux operating system (OS), then this book is for you.

kali linux hacking pdf: Kali Linux Revealed Raphaël Hertzog, Jim O'Gorman, Mati Aharoni, 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 hacking pdf: Hands-On Penetration Testing with Kali NetHunter Glen D. Singh, Sean-Philip Oriyano, 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 hacking pdf: 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

kali linux hacking pdf: Kali Linux Wireless Penetration Testing: Beginner's Guide Vivek Ramachandran, Cameron Buchanan, 2015-03-30 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.

kali linux hacking pdf: Beginning Ethical Hacking with Python Sanjib Sinha, 2016-12-25 Learn

the basics of ethical hacking and gain insights into the logic, algorithms, and syntax of Python. This book will set you up with a foundation that will help you understand the advanced concepts of hacking in the future. Learn Ethical Hacking with Python 3 touches the core issues of cyber security: in the modern world of interconnected computers and the Internet, security is increasingly becoming one of the most important features of programming. Ethical hacking is closely related to Python. For this reason this book is organized in three parts. The first part deals with the basics of ethical hacking; the second part deals with Python 3; and the third part deals with more advanced features of ethical hacking. What You Will Learn Discover the legal constraints of ethical hacking Work with virtual machines and virtualization Develop skills in Python 3 See the importance of networking in ethical hacking Gain knowledge of the dark web, hidden Wikipedia, proxy chains, virtual private networks, MAC addresses, and more Who This Book Is For Beginners wanting to learn ethical hacking alongside a modular object oriented programming language.

kali linux hacking pdf: Python for Offensive PenTest Hussam Khrais, 2018-04-26 Your one-stop guide to using Python, creating your own hacking tools, and making the most out of resources available for this programming language Key Features Comprehensive information on building a web application penetration testing framework using Python Master web application penetration testing using the multi-paradigm programming language Python Detect vulnerabilities in a system or application by writing your own Python scripts Book Description Python is an easy-to-learn and cross-platform programming language that has unlimited third-party libraries. Plenty of open source hacking tools are written in Python, which can be easily integrated within your script. This book is packed with step-by-step instructions and working examples to make you a skilled penetration tester. It is divided into clear bite-sized chunks, so you can learn at your own pace and focus on the areas of most interest to you. This book will teach you how to code a reverse shell and build an anonymous shell. You will also learn how to hack passwords and perform a privilege escalation on Windows with practical examples. You will set up your own virtual hacking environment in VirtualBox, which will help you run multiple operating systems for your testing environment. By the end of this book, you will have learned how to code your own scripts and mastered ethical hacking from scratch. What you will learn Code your own reverse shell (TCP and HTTP) Create your own anonymous shell by interacting with Twitter, Google Forms, and SourceForge Replicate Metasploit features and build an advanced shell Hack passwords using multiple techniques (API hooking, keyloggers, and clipboard hijacking) Exfiltrate data from your target Add encryption (AES, RSA, and XOR) to your shell to learn how cryptography is being abused by malware Discover privilege escalation on Windows with practical examples Countermeasures against most attacks Who this book is for This book is for ethical hackers; penetration testers; students preparing for OSCP, OSCE, GPEN, GXPN, and CEH; information security professionals; cybersecurity consultants; system and network security administrators; and programmers who are keen on learning all about penetration testing.

kali linux hacking pdf: Burp Suite Cookbook Sunny Wear, 2018-09-26 Get hands-on experience in using Burp Suite to execute attacks and perform web assessments Key FeaturesExplore the tools in Burp Suite to meet your web infrastructure security demandsConfigure Burp to fine-tune the suite of tools specific to the targetUse Burp extensions to assist with different technologies commonly found in application stacksBook Description Burp Suite is a Java-based platform for testing the security of your web applications, and has been adopted widely by professional enterprise testers. The Burp Suite Cookbook contains recipes to tackle challenges in determining and exploring vulnerabilities in web applications. You will learn how to uncover security flaws with various test cases for complex environments. After you have configured Burp for your environment, you will use Burp tools such as Spider, Scanner, Intruder, Repeater, and Decoder, among others, to resolve specific problems faced by pentesters. You will also explore working with various modes of Burp and then perform operations on the web. Toward the end, you will cover recipes that target specific test scenarios and resolve them using best practices. By the end of the book, you will be up and running with deploying Burp for securing web applications. What you will

learnConfigure Burp Suite for your web applicationsPerform authentication, authorization, business logic, and data validation testingExplore session management and client-side testingUnderstand unrestricted file uploads and server-side request forgeryExecute XML external entity attacks with BurpPerform remote code execution with BurpWho this book is for If you are a security professional, web pentester, or software developer who wants to adopt Burp Suite for applications security, this book is for you.

kali linux hacking pdf: Hands-On Penetration Testing on Windows Phil Bramwell, 2018-07-30 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

kali linux hacking pdf: The Hacker Playbook Peter Kim, 2014 Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans. Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the “game” of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style “plays,” this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing—including attacking different types of networks, pivoting through security controls, and evading antivirus software. From “Pregame” research to “The Drive” and “The Lateral Pass,” the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library—so there's no reason not to get in the game.

kali linux hacking pdf: Hacking- The art Of Exploitation J. Erickson, 2018-03-06 This text introduces the spirit and theory of hacking as well as the science behind it all; it also provides some core techniques and tricks of hacking so you can think like a hacker, write your own hacks or thwart potential system attacks.

kali linux hacking pdf: *Advanced Penetration Testing* Wil Allsopp, 2017-02-27 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 hacking pdf: *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.

kali linux hacking pdf: Kali Linux Penetration Testing Bible Gus Khawaja, 2021-04-26 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

kali linux hacking pdf: Kali Linux Web Penetration Testing Cookbook Gilberto Nájera-Gutiérrez, 2016-02-29 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.

kali linux hacking pdf: Hacking with Kali Linux Ramon Nastase, 2018-10-15 Ever wondered how a Hacker thinks? Or how you could become a Hacker? This book will show you how Hacking

works. You will have a chance to understand how attackers gain access to your systems and steal information. Also, you will learn what you need to do in order to protect yourself from all kind of hacking techniques. Structured on 10 chapters, all about hacking, this is in short what the book covers in its pages: The type of hackers How the process of Hacking works and how attackers cover their traces How to install and use Kali Linux The basics of CyberSecurity All the information on malware and cyber attacks How to scan the servers and the network WordPress security & Hacking 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 own security Get this book NOW. Hacking is real, and many people know how to do it. You can protect yourself from cyber attacks by being informed and learning how to secure your computer and other devices. Tags: Computer Security, Hacking, CyberSecurity, Cyber Security, Hacker, Malware, Kali Linux, Security, Hack, Hacking with Kali Linux, Cyber Attack, VPN, Cryptography

kali linux hacking pdf: Learn Ethical Hacking from Scratch Zaid Sabih, 2018-07-31 Learn how to hack systems like black hat hackers and secure them like security experts Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to secure systems from hackers Book Description This book starts with the basics of ethical hacking, how to practice hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking, where you will see how to test the security of wired and wireless networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks. You will also get the hang of post-exploitation techniques, including remotely controlling and interacting with the systems that you compromised. Towards the end of the book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the different fields and types of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how to hack and test the security of systems like professional hackers and security experts.

kali linux hacking pdf: Practical IoT Hacking Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods, 2021-03-23 The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to: • Write a DICOM service scanner as an NSE module • Hack a microcontroller through the UART and SWD interfaces • Reverse engineer firmware and analyze mobile companion apps • Develop an NFC fuzzer using Proxmark3 • Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team

member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

kali linux hacking pdf: *Black Hat Go* Tom Steele, Chris Patten, Dan Kottmann, 2020-02-04 Like the best-selling Black Hat Python, Black Hat Go explores the darker side of the popular Go programming language. This collection of short scripts will help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset. Black Hat Go explores the darker side of Go, the popular programming language revered by hackers for its simplicity, efficiency, and reliability. It provides an arsenal of practical tactics from the perspective of security practitioners and hackers to help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset, all using the power of Go. You'll begin your journey with a basic overview of Go's syntax and philosophy and then start to explore examples that you can leverage for tool development, including common network protocols like HTTP, DNS, and SMB. You'll then dig into various tactics and problems that penetration testers encounter, addressing things like data pilfering, packet sniffing, and exploit development. You'll create dynamic, pluggable tools before diving into cryptography, attacking Microsoft Windows, and implementing steganography. You'll learn how to: Make performant tools that can be used for your own security projects Create usable tools that interact with remote APIs Scrape arbitrary HTML data Use Go's standard package, net/http, for building HTTP servers Write your own DNS server and proxy Use DNS tunneling to establish a C2 channel out of a restrictive network Create a vulnerability fuzzer to discover an application's security weaknesses Use plug-ins and extensions to future-proof productsBuild an RC2 symmetric-key brute-forcer Implant data within a Portable Network Graphics (PNG) image. Are you ready to add to your arsenal of security tools? Then let's Go!

kali linux hacking pdf: The Basics of Web Hacking Josh Pauli, 2013-06-18 The Basics of Web Hacking introduces you to a tool-driven process to identify the most widespread vulnerabilities in Web applications. No prior experience is needed. Web apps are a path of least resistance that can be exploited to cause the most damage to a system, with the lowest hurdles to overcome. This is a perfect storm for beginning hackers. The process set forth in this book introduces not only the theory and practical information related to these vulnerabilities, but also the detailed configuration and usage of widely available tools necessary to exploit these vulnerabilities. The Basics of Web Hacking provides a simple and clean explanation of how to utilize tools such as Burp Suite, sqlmap, and Zed Attack Proxy (ZAP), as well as basic network scanning tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more. Dr. Josh Pauli teaches software security at Dakota State University and has presented on this topic to the U.S. Department of Homeland Security, the NSA, BlackHat Briefings, and Defcon. He will lead you through a focused, three-part approach to Web security, including hacking the server, hacking the Web app, and hacking the Web user. With Dr. Pauli's approach, you will fully understand the what/where/why/how of the most widespread Web vulnerabilities and how easily they can be exploited with the correct tools. You will learn how to set up a safe environment to conduct these attacks, including an attacker Virtual Machine (VM) with all necessary tools and several known-vulnerable Web application VMs that are widely available and maintained for this very purpose. Once you complete the entire process, not only will you be prepared to test for the most damaging Web exploits, you will also be prepared to conduct more advanced Web hacks that mandate a strong base of knowledge. - Provides a simple and clean approach to Web hacking, including hands-on examples and exercises that are designed to teach you how to hack the server, hack the Web app, and hack the Web user - Covers the most significant new tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more! - Written by an author who works in the field as a penetration tester and who teaches Web security classes at Dakota State University

kali linux hacking pdf: Hacking with Kali Linux: a Guide to Ethical Hacking Grzegorz Nowak, 2019-10-22 ▶ 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. □ When you are ready to learn more about hacking with Kali Linux and how this can benefit your own network and computer, make sure to check out this guidebook to get started!

kali linux hacking pdf: *The Web Application Hacker's Handbook* Dafydd Stuttard, Marcus Pinto, 2011-03-16 This book is a practical guide to discovering and exploiting security flaws in web applications. The authors explain each category of vulnerability using real-world examples, screen shots and code extracts. The book is extremely practical in focus, and describes in detail the steps involved in detecting and exploiting each kind of security weakness found within a variety of applications such as online banking, e-commerce and other web applications. The topics covered include bypassing login mechanisms, injecting code, exploiting logic flaws and compromising other users. Because every web application is different, attacking them entails bringing to bear various general principles, techniques and experience in an imaginative way. The most successful hackers go beyond this, and find ways to automate their bespoke attacks. This handbook describes a proven methodology that combines the virtues of human intelligence and computerized brute force, often with devastating results. The authors are professional penetration testers who have been involved in web application security for nearly a decade. They have presented training courses at the Black Hat security conferences throughout the world. Under the alias PortSwigger, Dafydd developed the popular Burp Suite of web application hack tools.

kali linux hacking pdf: Linux For Dummies Richard Blum, 2009-07-17 One of the fastest ways to learn Linux is with this perennial favorite Eight previous top-selling editions of Linux For Dummies can't be wrong. If you've been wanting to migrate to Linux, this book is the best way to get there. Written in easy-to-follow, everyday terms, Linux For Dummies 9th Edition gets you started by concentrating on two distributions of Linux that beginners love: the Ubuntu LiveCD distribution and the gOS Linux distribution, which comes pre-installed on Everex computers. The book also covers the full Fedora distribution. Linux is an open-source operating system and a low-cost or free alternative to Microsoft Windows; of numerous distributions of Linux, this book covers Ubuntu Linux, Fedora Core Linux, and gOS Linux, and includes them on the DVD. Install new open source software via Synaptic or RPM package managers Use free software to browse the Web, listen to music, read e-mail, edit photos, and even run Windows in a virtualized environment Get acquainted with the Linux command line If you want to get a solid foundation in Linux, this popular, accessible book is for you. Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

kali linux hacking pdf: *Hacking* John Medicine, 2020-02-09 Do you want to learn how to set up a new network for your home or business place and get the best performance of your network? Are you worried about the security structure of your network and want to prevent all forms of attacks on your system? If so then keep reading. The various forms of internet communication have changed the whole concept of communication across a long distance. Networking has adapted the concepts of wireless functioning which have helped in wiping out various redundancies. The wired form of network is still in use owing to its special features and working capabilities. Networking is a complex concept and if done right it can do wonders. Having a brief overview of the networking concepts is very essential for setting up a new network or for improving the functionality of an existing network. It is not at all easy to constantly look out for the various forms of threats that are always ready to attack your system of network. It is your prime duty to analyze your network and check out for the various loopholes that are present within the system. Failing to do so might result in serious loss data and security breach. For having a proper idea about the security threats, it is crucial to learn about the process of hacking in the first place. When you have proper knowledge about the complete process of hacking, you can easily trace out the threats for your system and also improve the security measures for the same. You can perform various functions with the help of Kali Linux. It not only helps in hacking but also provides the users with various tools that can help in testing the networks for security vulnerabilities. It is a very process to set up the OS and can be installed on any form of system. There are various types of cyber-attacks and as the owner of an organization you are required to have proper knowledge about the same. This will help you in planning out preventive measures for the future attacks. As every disease comes with an antidote, cyber-attacks also come with antivirus software for preventing them from attacking the systems. You will learn: The basic format of networking The successful networking processes The master controller who holds all necessary information required by the recipient The necessary components of networking The types of networks Wireless Networking Peer to Peer Connection OSI Model Network Mode Security Circuit and Packet Switching FTP - File Transfer Protocol Network structure and management Concepts of cyber security How to implement security measures Bash and Python Scripting Wireless network security Types of attacks Firewall security Cryptography and Network security Penetration Testing ...and more! You need to start from the beginning in order to setup a proper security system or want to learn how to hack networks! The chapters of this book have been arranged in a unique way that will provide you with the answers to all your questions regarding hacking and security of network. So, if you are interested in the various aspects of Kali Linux along with network security, and want to feel like a Master of Hacking, Scroll up and click the Buy Now button!

kali linux hacking pdf: Hacking with Kali Linux Daniel Howard, 2019-11-11 If you are searching for the fastest way to learn the secrets of a professional hacker, then keep reading. You are about to begin a journey into the deepest areas of the web, which will lead you to understand perfectly the most effective strategies to hack any system you want, even if you have zero experience and you are brand new to programming. In this book, Daniel Howard has condensed all the knowledge you need in a simple and practical way, with real-world examples, step-by-step instructions and tips from his experience. Kali Linux is an open-source project, worldwide recognized as the most powerful tool for computer security and penetration testing, thanks to its large number of dedicated functions which will be discussed in detail. Anyone should read the information inside this book, at least to identify any potential security issue and prevent serious consequences for his own security or even his privacy. You need to stay a step ahead of any criminal hacker, which is exactly where you will be after reading Hacking with Kali Linux. Moreover, don't forget that hacking is absolutely not necessarily associated to a criminal activity. In fact, ethical hacking is becoming one of the most requested and well-paid positions in every big company all around the world. If you are a student or a professional interested in developing a career in this world, this book will be your best guide. Here's just a tiny fraction of what you'll discover: Different types of hacking attacks What is ethical hacking How to crack any computer and any network system, accessing all the data you want How to master the Linux operating system and its command

line How to use Kali Linux for hacking and penetration testing Kali Linux port scanning strategies Little known cryptography techniques Computer networks' vulnerabilities and the basics of cybersecurity How to identify suspicious signals and prevent any external attack against your own device How to use VPNs and firewalls If you are ready to access the hidden world of hacking, then click the BUY button and get your copy!

kali linux hacking pdf: The Linux Command Line, 2nd Edition William Shotts, 2019-03-05 You've experienced the shiny, point-and-click surface of your Linux computer--now dive below and explore its depths with the power of the command line. The Linux Command Line takes you from your very first terminal keystrokes to writing full programs in Bash, the most popular Linux shell (or command line). Along the way you'll learn the timeless skills handed down by generations of experienced, mouse-shunning gurus: file navigation, environment configuration, command chaining, pattern matching with regular expressions, and more. In addition to that practical knowledge, author William Shotts reveals the philosophy behind these tools and the rich heritage that your desktop Linux machine has inherited from Unix supercomputers of yore. As you make your way through the book's short, easily-digestible chapters, you'll learn how to: • Create and delete files, directories, and symlinks • Administer your system, including networking, package installation, and process management • Use standard input and output, redirection, and pipelines • Edit files with Vi, the world's most popular text editor • Write shell scripts to automate common or boring tasks • Slice and dice text files with cut, paste, grep, patch, and sed Once you overcome your initial shell shock, you'll find that the command line is a natural and expressive way to communicate with your computer. Just don't be surprised if your mouse starts to gather dust.

kali linux hacking pdf: *Wireshark for Security Professionals* Jessey Bullock, Jeff T. Parker, 2017-03-20 Master Wireshark to solve real-world security problems If you don’t already use Wireshark for a wide range of information security tasks, you will after this book. Mature and powerful, Wireshark is commonly used to find root cause of challenging network issues. This book extends that power to information security professionals, complete with a downloadable, virtual lab environment. Wireshark for Security Professionals covers both offensive and defensive concepts that can be applied to essentially any InfoSec role. Whether into network security, malware analysis, intrusion detection, or penetration testing, this book demonstrates Wireshark through relevant and useful examples. Master Wireshark through both lab scenarios and exercises. Early in the book, a virtual lab environment is provided for the purpose of getting hands-on experience with Wireshark. Wireshark is combined with two popular platforms: Kali, the security-focused Linux distribution, and the Metasploit Framework, the open-source framework for security testing. Lab-based virtual systems generate network traffic for analysis, investigation and demonstration. In addition to following along with the labs you will be challenged with end-of-chapter exercises to expand on covered material. Lastly, this book explores Wireshark with Lua, the light-weight programming language. Lua allows you to extend and customize Wireshark’s features for your needs as a security professional. Lua source code is available both in the book and online. Lua code and lab source code are available online through GitHub, which the book also introduces. The book’s final two chapters greatly draw on Lua and TShark, the command-line interface of Wireshark. By the end of the book you will gain the following: Master the basics of Wireshark Explore the virtual w4sp-lab environment that mimics a real-world network Gain experience using the Debian-based Kali OS among other systems Understand the technical details behind network attacks Execute exploitation and grasp offensive and defensive activities, exploring them through Wireshark Employ Lua to extend Wireshark features and create useful scripts To sum up, the book content, labs and online material, coupled with many referenced sources of PCAP traces, together present a dynamic and robust manual for information security professionals seeking to leverage Wireshark.

kali linux hacking pdf: Ethical Hacking with Kali Linux Made Easy Mohamad Mahjoub, 2020-09-22 The book examines various penetration testing concepts and techniques employed in the modern computing world. It will take you from a beginner to advanced level. We will discuss various topics ranging from traditional to modern ones, such as Networking security, Linux security, Web

Applications structure and security, Mobile Applications architecture and security, Hardware security, and the hot topic of IoT security. At the end of the book, I will share with you some real attacks. The layout of the book is easy to walk-through. My purpose is to present you with case exposition and show you actual attacks, while utilizing a large set of KALI tools (Enumeration, Scanning, Exploitation, Persistence Access, Reporting and Social Engineering tools) in order to get you started quickly. Before jumping into penetration testing, you will first learn how to set up your own lab and install the needed software to get you started. All the attacks explained in this book are launched against real devices, and nothing is theoretical. The book will demonstrate how to fully control victims' devices such as servers, workstations, and mobile phones. The book can also be interesting to those looking for quick hacks such as controlling victim's camera, screen, mobile contacts, emails and SMS messages. WHAT WILL YOU LEARN?Learn simplified ethical hacking techniques from scratchPerform an actual Mobile attackMaster 2 smart techniques to crack into wireless networksLearn more than 9 ways to perform LAN attacksLearn Linux basicsLearn 10+ web application attacksLearn more than 5 proven methods of Social Engineering attacksObtain 20+ skills any penetration tester needs to succeedMake better decisions on how to protect your applications and networkUpgrade your information security skills for a new job or career changeLearn how to write a professional penetration testing reportWHO IS THIS BOOK FOR?Anyone who wants to learn how to secure their systems from hackerAnyone who wants to learn how hackers can attack their computer systemsAnyone looking to become a penetration tester (From zero to hacker)Computer Science, Computer Security, and Computer Engineering StudentsWAIT! THERE IS MOREYou can as well enjoy the JUICY BONUS section at the end of the book, which shows you how to setup useful portable Pentest Hardware Tools that you can employ in your attacks. The book comes with a complete Github repository containing all the scripts and commands needed. I have put my years of experience into this book by trying to answer many of the questions I had during my journey of learning. I have as well took the feedback and input of many of my students, peers, and professional figures.Hack Ethically !

kali linux hacking pdf: 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!

kali linux hacking pdf: Nmap: Network Exploration and Security Auditing Cookbook Paulino Calderon, 2017-05-26 Over 100 practical recipes related to network and application security auditing using the powerful Nmap About This Book Learn through practical recipes how to use Nmap for a wide range of tasks for system administrators and penetration testers. Learn the latest and most useful features of Nmap and the Nmap Scripting Engine. Learn to audit the security of networks, web applications, databases, mail servers, Microsoft Windows servers/workstations and even ICS systems. Learn to develop your own modules for the Nmap Scripting Engine. Become familiar with Lua programming. 100% practical tasks, relevant and explained step-by-step with exact commands and optional arguments description Who This Book Is For The book is for anyone who wants to master Nmap and its scripting engine to perform real life security auditing checks for system administrators and penetration testers. This book is also recommended to anyone looking to learn about network security auditing. Finally, novice Nmap users will also learn a lot from this book as it covers several advanced internal aspects of Nmap and related tools. What You Will Learn Learn

about Nmap and related tools, such as Ncat, Ncrack, Ndiff, Zenmap and the Nmap Scripting Engine Master basic and advanced techniques to perform port scanning and host discovery Detect insecure configurations and vulnerabilities in web servers, databases, and mail servers Learn how to detect insecure Microsoft Windows workstations and scan networks using the Active Directory technology Learn how to safely identify and scan critical ICS/SCADA systems Learn how to optimize the performance and behavior of your scans Learn about advanced reporting Learn the fundamentals of Lua programming Become familiar with the development libraries shipped with the NSE Write your own Nmap Scripting Engine scripts In Detail This is the second edition of 'Nmap 6: Network Exploration and Security Auditing Cookbook'. A book aimed for anyone who wants to master Nmap and its scripting engine through practical tasks for system administrators and penetration testers. Besides introducing the most powerful features of Nmap and related tools, common security auditing tasks for local and remote networks, web applications, databases, mail servers, Microsoft Windows machines and even ICS SCADA systems are explained step by step with exact commands and argument explanations. The book starts with the basic usage of Nmap and related tools like Ncat, Ncrack, Ndiff and Zenmap. The Nmap Scripting Engine is thoroughly covered through security checks used commonly in real-life scenarios applied for different types of systems. New chapters for Microsoft Windows and ICS SCADA systems were added and every recipe was revised. This edition reflects the latest updates and hottest additions to the Nmap project to date. The book will also introduce you to Lua programming and NSE script development allowing you to extend further the power of Nmap. Style and approach This book consists of practical recipes on network exploration and security auditing techniques, enabling you to get hands-on experience through real life scenarios.

kali linux hacking pdf: *Black Hat Python, 2nd Edition* Justin Seitz, Tim Arnold, 2021-04-13 Fully-updated for Python 3, the second edition of this worldwide bestseller (over 100,000 copies sold) explores the stealthier side of programming and brings you all new strategies for your hacking projects. When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security analysts. In Black Hat Python, 2nd Edition, you'll explore the darker side of Python's capabilities—writing network sniffers, stealing email credentials, brute forcing directories, crafting mutation fuzzers, infecting virtual machines, creating stealthy trojans, and more. The second edition of this bestselling hacking book contains code updated for the latest version of Python 3, as well as new techniques that reflect current industry best practices. You'll also find expanded explanations of Python libraries such as ctypes, struct, lxml, and BeautifulSoup, and dig deeper into strategies, from splitting bytes to leveraging computer-vision libraries, that you can apply to future hacking projects. You'll learn how to: • Create a trojan command-and-control using GitHub • Detect sandboxing and automate common malware tasks, like keylogging and screenshotting • Escalate Windows privileges with creative process control • Use offensive memory forensics tricks to retrieve password hashes and inject shellcode into a virtual machine • Extend the popular Burp Suite web-hacking tool • Abuse Windows COM automation to perform a man-in-the-browser attack • Exfiltrate data from a network most sneakily When it comes to offensive security, your ability to create powerful tools on the fly is indispensable. Learn how with the second edition of Black Hat Python. New to this edition: All Python code has been updated to cover Python 3 and includes updated libraries used in current Python applications. Additionally, there are more in-depth explanations of the code and the programming techniques have been updated to current, common tactics. Examples of new material that you'll learn include how to sniff network traffic, evade anti-virus software, brute-force web applications, and set up a command-and-control (C2) system using GitHub.

Back to Home: https://a.comtex-nj.com