the basics of hacking and penetration testing pdf

the basics of hacking and penetration testing pdf serves as an essential resource for anyone interested in understanding the fundamental concepts and practical approaches to cybersecurity. This guide comprehensively covers the methodologies used by ethical hackers and penetration testers to identify and exploit vulnerabilities within computer systems and networks. Understanding the basics of hacking and penetration testing equips professionals with the necessary skills to defend against malicious attacks and strengthen organizational security postures. This article provides an in-depth overview of key topics such as ethical hacking principles, types of penetration testing, essential tools, and legal considerations. Whether you are a beginner or an experienced security enthusiast, mastering these basics through a well-structured PDF guide can enhance your expertise in safeguarding digital environments. The following sections will delve into the core areas of hacking and penetration testing to provide a clear roadmap for learners and practitioners alike.

Understanding Hacking and Its Types

Hacking refers to the process of exploiting weaknesses in computer systems, networks, or applications to gain unauthorized access or perform unauthorized actions. In the context of cybersecurity, understanding hacking involves differentiating between malicious activities and ethical hacking practices aimed at improving security. The basics of hacking and penetration testing pdf often start by explaining various hacker classifications and attack vectors used to compromise systems.

Types of Hackers

Hackers are generally categorized based on their intent and authorization level. The most common types include:

- **Black Hat Hackers:** Individuals who exploit vulnerabilities for malicious purposes such as theft, damage, or disruption.

- **White Hat Hackers:** Ethical hackers authorized to test systems and identify security flaws to help organizations improve their defenses.
- **Gray Hat Hackers:** Hackers who may violate laws or ethical standards but do not have malicious intent, sometimes exposing vulnerabilities publicly without permission.

Common Hacking Methods

Understanding the common hacking methods is crucial for anyone learning the basics of hacking and penetration testing pdf. These methods include:

- Phishing and Social Engineering
- SQL Injection
- Cross-Site Scripting (XSS)
- Denial of Service (DoS) Attacks
- Man-in-the-Middle (MitM) Attacks

The Role of Penetration Testing in Cybersecurity

Penetration testing, often called pen testing, is a proactive security practice aimed at simulating cyberattacks to discover vulnerabilities before malicious hackers can exploit them. The basics of hacking and penetration testing pdf typically emphasize how penetration tests help organizations identify weaknesses in their infrastructure, applications, and human factors.

Types of Penetration Testing

There are several types of penetration testing, each targeting different aspects of security:

- **Black Box Testing:** Testing without prior knowledge of the system, simulating an external attacker’s perspective.
- **White Box Testing:** Testing with full knowledge of the system, including source code and architecture.
- **Gray Box Testing:** Partial knowledge of the system is available to the tester, combining elements of both black and white box testing.

Benefits of Penetration Testing

Penetration testing provides several benefits, such as:

- Identifying and mitigating security vulnerabilities.
- Testing the effectiveness of security controls.
- Enhancing compliance with industry regulations.
- Improving incident response capabilities.

Essential Tools for Hacking and Penetration Testing

The basics of hacking and penetration testing pdf often include a review of the most widely used tools that ethical hackers and penetration testers rely on to conduct assessments. These tools facilitate information gathering, vulnerability scanning, exploitation, and reporting.

Information Gathering Tools

Reconnaissance is a critical phase in penetration testing, and several tools assist in this stage:

- **Nmap:** Network scanner used to discover hosts and services on a computer network.
- **Recon-ng:** A reconnaissance framework with modules for gathering intelligence.
- **Maltego:** Tool for visualizing relationships and links between data points.

Vulnerability Scanning and Exploitation Tools

After gathering information, testers utilize specialized tools to find and exploit vulnerabilities:

- **Metasploit Framework:** A powerful exploitation tool used to develop and execute exploit code.
- **Burp Suite:** Web vulnerability scanner and proxy tool.
- **OpenVAS:** Open-source vulnerability scanner for network security assessments.

Common Techniques and Methodologies

The basics of hacking and penetration testing pdf detail various techniques and methodologies that practitioners employ during assessments. These structured approaches ensure thorough evaluation and consistent results.

Phases of Penetration Testing

Penetration testing typically follows a systematic process that includes the following phases:

1. **Planning and Preparation:** Defining scope, rules of engagement, and objectives.
2. **Reconnaissance:** Collecting information about the target.
3. **Scanning:** Identifying live hosts, open ports, and services.
4. **Exploitation:** Attempting to exploit discovered vulnerabilities.
5. **Post-Exploitation:** Assessing the impact and maintaining access.
6. **Reporting:** Documenting findings and recommending mitigations.

Social Engineering Techniques

Social engineering remains a significant component of hacking and penetration testing. It involves manipulating individuals to gain access or sensitive information. Common tactics include:

- Phishing emails
- Pretexting
- Baiting
- Tailgating

Legal and Ethical Considerations

The basics of hacking and penetration testing pdf emphasize the importance of adhering to legal and ethical standards. Unauthorized hacking is illegal and punishable by law, whereas ethical hacking requires explicit permission from the system owner.

Authorization and Scope

Penetration testers must obtain written authorization defining the scope and limits of their activities. This protects both the tester and the organization from legal repercussions.

Compliance and Regulations

Various laws and industry standards govern cybersecurity practices, including:

- Computer Fraud and Abuse Act (CFAA)
- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)

Learning Resources and Using PDFs Effectively

PDF guides on the basics of hacking and penetration testing provide structured and accessible material for learners. These documents often include theoretical explanations, practical exercises, and tool tutorials.

Advantages of PDF Learning Materials

PDFs offer several benefits for cybersecurity education:

- Portability and offline access
- Consistent formatting and ease of annotation
- Comprehensive coverage of topics
- Integration of images, diagrams, and code snippets

Maximizing Learning with PDFs

To effectively use the basics of hacking and penetration testing pdf resources, learners should:

- Follow along with practical labs and simulations.
- Cross-reference with updated online resources and communities.

- Practice ethical hacking in controlled environments.
- Regularly review and update knowledge based on emerging threats.

Frequently Asked Questions

What is the 'Basics of Hacking and Penetration Testing' PDF about?

The 'Basics of Hacking and Penetration Testing' PDF is a resource that introduces fundamental concepts, tools, and techniques used in ethical hacking and penetration testing to identify and fix security vulnerabilities.

Is the 'Basics of Hacking and Penetration Testing' PDF suitable for beginners?

Yes, this PDF is designed for beginners and covers foundational topics to help newcomers understand the principles and methodologies of ethical hacking and penetration testing.

What topics are typically covered in the 'Basics of Hacking and Penetration Testing' PDF?

Common topics include network scanning, vulnerability assessment, exploitation techniques, post-exploitation, reporting, and the use of popular tools like Nmap, Metasploit, and Wireshark.

Can I use the 'Basics of Hacking and Penetration Testing' PDF for preparing for certification exams?

Yes, the content is useful for foundational knowledge required in certifications like CEH (Certified Ethical Hacker) and OSCP (Offensive Security Certified Professional), though additional study materials may be needed.

Are there practical exercises included in the 'Basics of Hacking and Penetration Testing' PDF?

Many versions of the PDF include hands-on labs and exercises to practice penetration testing techniques in controlled environments.

Is it legal to use the knowledge from the 'Basics of Hacking and Penetration Testing' PDF on any network?

No, ethical hacking must always be conducted with proper authorization. Using hacking techniques on unauthorized networks is illegal and unethical.

Where can I find a reliable 'Basics of Hacking and Penetration Testing' PDF?

Reliable PDFs can often be found through official websites of cybersecurity educators, reputable online bookstores, or academic institutions offering cybersecurity courses.

Does the 'Basics of Hacking and Penetration Testing' PDF cover the latest hacking tools and techniques?

While it covers foundational tools and techniques, users should supplement the PDF with up-to-date resources as cybersecurity threats and tools evolve rapidly.

What software tools are recommended in the 'Basics of Hacking and Penetration Testing' PDF?

Tools like Nmap for scanning, Metasploit for exploitation, Wireshark for traffic analysis, and Burp Suite for web application testing are commonly recommended.

How can the 'Basics of Hacking and Penetration Testing' PDF help improve cybersecurity skills?

By providing a structured introduction to hacking methodologies, it helps learners understand how attackers think and operate, enabling them to better secure systems against vulnerabilities.

Additional Resources

1. *Hacking: The Art of Exploitation, 2nd Edition*
This book by Jon Erickson offers a comprehensive introduction to the fundamentals of hacking and penetration testing. It covers topics such as programming, network communications, and exploitation techniques, blending theory with practical examples. Readers gain a deep understanding of how vulnerabilities work and how hackers exploit them, making it ideal for beginners and intermediate learners.

2. *Penetration Testing: A Hands-On Introduction to Hacking*
Written by Georgia Weidman, this book provides a practical approach to learning penetration testing. It covers setting up a lab environment, using essential tools, and performing various types of attacks like network, web, and wireless penetration tests. The hands-on exercises make it a great resource for those looking to build foundational skills.

3. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*
By Patrick Engebretson, this book is designed for beginners who want a straightforward introduction to ethical hacking. It outlines the key phases of penetration testing, including reconnaissance, scanning, exploitation, and reporting. The book also includes practical labs and exercises to reinforce learning.

4. *Metasploit: The Penetration Tester’s Guide*

This guide, authored by David Kennedy and others, focuses on using the Metasploit Framework, a powerful tool for penetration testing. Readers learn how to identify vulnerabilities, write exploits, and automate attacks with Metasploit. The book balances theory with practical application, making it useful for both novices and experienced testers.

5. *Gray Hat Hacking: The Ethical Hacker's Handbook*
This comprehensive text covers a broad range of hacking topics from an ethical perspective. It explains how to perform penetration tests, identify vulnerabilities, and use various hacking tools. With contributions from multiple experts, the book provides real-world scenarios and advanced techniques for learners who want to deepen their knowledge.

6. *Network Security Assessment: Know Your Network*
By Chris McNab, this book focuses on assessing network security through penetration testing techniques. It guides readers through the process of discovering vulnerabilities, exploiting weaknesses, and evaluating security controls. The clear explanations and practical examples help readers understand the complexities of network security assessments.

7. *Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*
Authors Dafydd Stuttard and Marcus Pinto delve into web application security, explaining how to identify and exploit common vulnerabilities. The book covers tools and methodologies essential for penetration testers focusing on web apps. It is a valuable resource for understanding the security challenges unique to web environments.

8. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*
Though focused on malware, this book by Michael Sikorski and Andrew Honig is useful for penetration testers interested in understanding the threats they face. It teaches how to analyze, dissect, and understand malware behavior using practical techniques. This knowledge helps testers anticipate and defend against sophisticated attacks.

9. *Social Engineering: The Science of Human Hacking*
Christopher Hadnagy's book explores the human element of security vulnerabilities through social engineering tactics. It explains psychological principles used by attackers to manipulate individuals and gain unauthorized access. This text is crucial for penetration testers who want to understand and defend against social engineering attacks.

The Basics Of Hacking And Penetration Testing Pdf

The Basics of Hacking and Penetration Testing PDF

Ebook Name: Cybersecurity Fundamentals: A Practical Guide to Ethical Hacking and Penetration Testing

Contents Outline:

Introduction: What is hacking and penetration testing? Ethical considerations and legal implications.
Chapter 1: Networking Fundamentals: IP addresses, TCP/IP model, network topologies, ports and protocols.
Chapter 2: Reconnaissance and Information Gathering: Passive and active reconnaissance

techniques, footprinting, social engineering.
Chapter 3: Vulnerability Assessment: Identifying system weaknesses, using vulnerability scanners, understanding CVEs.
Chapter 4: Exploitation Techniques: Understanding exploit development, buffer overflows, SQL injection, cross-site scripting (XSS).
Chapter 5: Penetration Testing Methodologies: Different penetration testing approaches (black box, white box, grey box), reporting.
Chapter 6: Post-Exploitation and Privilege Escalation: Maintaining access, gaining higher privileges, lateral movement.
Chapter 7: Security Hardening and Mitigation: Implementing security best practices, patching vulnerabilities, intrusion detection systems (IDS).
Conclusion: Recap of key concepts, future trends in cybersecurity, and resources for further learning.

The Basics of Hacking and Penetration Testing: A Comprehensive Guide

Introduction: Understanding the Landscape of Ethical Hacking and Penetration Testing

The terms "hacking" and "penetration testing" are often used interchangeably, but there's a crucial distinction. Hacking, in its broadest sense, refers to gaining unauthorized access to a computer system or network. This can range from simple pranks to sophisticated attacks aimed at stealing data, disrupting services, or causing financial damage. Penetration testing, on the other hand, is a legal and ethical process that simulates real-world hacking attacks to identify vulnerabilities in a system before malicious actors can exploit them. Ethical hackers, also known as penetration testers or "white hat" hackers, use their skills to proactively strengthen security.

This guide will focus on the fundamentals of penetration testing, covering the essential concepts and techniques used by ethical hackers to assess and improve cybersecurity posture. It's crucial to emphasize the ethical and legal ramifications. Unauthorized access to any system, regardless of intent, is illegal and carries severe consequences. This guide is intended for educational purposes only and should not be used to perform illegal activities.

Chapter 1: Networking Fundamentals – The Foundation of Cybersecurity

Understanding computer networks is paramount for any aspiring penetration tester. This chapter will cover essential concepts such as:

IP Addresses: The unique numerical identifier assigned to every device connected to a network (IPv4 and IPv6). Knowing how IP addresses are structured and used is fundamental to network mapping and reconnaissance.
TCP/IP Model: The core protocol suite governing how data is transmitted across networks. Understanding the different layers (application, transport, network, link, physical) is crucial to analyzing network traffic and identifying vulnerabilities.
Network Topologies: Different ways networks can be structured (bus, star, ring, mesh). Understanding these topologies helps in visualizing network architecture and identifying potential weak points.
Ports and Protocols: Ports are numerical identifiers used by applications to communicate over a network. Protocols define the rules and standards for communication (e.g., HTTP, HTTPS, FTP, SMTP). Knowing which ports are used by common services is essential for vulnerability scanning and exploitation.

A solid grasp of these networking fundamentals is the cornerstone for effective penetration testing. Without it, navigating network infrastructure and identifying vulnerabilities becomes extremely difficult.

Chapter 2: Reconnaissance and Information Gathering – The Art of Intelligence Gathering

Reconnaissance is the initial phase of penetration testing, where the tester gathers information about the target system. This involves both passive and active techniques:

Passive Reconnaissance: This involves gathering information publicly available online, such as website content, social media profiles, company directories, and news articles. This is a crucial step to building a profile of the target and identifying potential entry points.
Active Reconnaissance: This involves directly interacting with the target system to gather information. This might involve scanning for open ports, identifying running services, and probing for vulnerabilities. It's essential to be mindful of legal and ethical boundaries during active reconnaissance, as unauthorized scanning can be illegal.
Footprinting: This involves systematically collecting information about the target's network infrastructure, including IP addresses, domain names, and network services. Various tools, such as Nmap and traceroute, are used for footprinting.
Social Engineering: This involves manipulating individuals to reveal sensitive information. While ethically grey, understanding social engineering techniques is crucial for penetration testers to identify human vulnerabilities within an organization's security posture.

Effective reconnaissance lays the groundwork for successful penetration testing. The more information a tester gathers, the better they can understand the target's weaknesses and develop effective attack strategies.

Chapter 3: Vulnerability Assessment – Identifying Weak Points

Vulnerability assessment involves identifying security weaknesses in a system. This can be done manually or using automated tools:

Manual Vulnerability Assessment: This involves meticulously examining the system's code, configuration files, and network infrastructure for weaknesses. This method requires a deep understanding of security principles and programming.
Automated Vulnerability Scanners: These tools automate the process of identifying vulnerabilities. Popular scanners include Nessus, OpenVAS, and QualysGuard. These tools scan for known vulnerabilities, often based on publicly available databases of Common Vulnerabilities and Exposures (CVEs).
Understanding CVEs: CVEs are standardized identifiers for publicly known security vulnerabilities. Understanding CVEs is crucial for prioritizing vulnerabilities and developing appropriate mitigation strategies.

Vulnerability assessment is a critical step in penetration testing, as it provides a clear picture of the system's weaknesses before attempting exploitation.

Chapter 4: Exploitation Techniques – Turning Vulnerabilities into Access

Exploitation involves taking advantage of identified vulnerabilities to gain unauthorized access to a system. This chapter covers various techniques, including:

Understanding Exploit Development: This involves writing custom code to exploit a specific vulnerability. This requires advanced programming skills and a deep understanding of system architecture.
Buffer Overflows: A common vulnerability where an application fails to properly handle input data, leading to a buffer overflow that can be exploited to execute arbitrary code.
SQL Injection: A technique that involves injecting malicious SQL code into a web application to gain unauthorized access to the database.
Cross-Site Scripting (XSS): A type of vulnerability where malicious scripts are injected into a website, allowing attackers to steal user data or hijack sessions.

Exploitation techniques require advanced technical skills and a deep understanding of system vulnerabilities. Ethical hackers must use these techniques responsibly and only within the scope of authorized penetration testing engagements.

Chapter 5: Penetration Testing Methodologies – Different

Approaches

Penetration testing can be performed using different methodologies:

Black Box Testing: The tester has no prior knowledge of the target system. This simulates a real-world attack scenario.
White Box Testing: The tester has full knowledge of the target system, including its architecture, code, and configuration.
Grey Box Testing: The tester has some knowledge of the target system, such as network diagrams or partial access.

Each methodology has its strengths and weaknesses, and the choice depends on the specific goals and scope of the penetration test. The methodology also dictates the reporting process – a crucial aspect to show the findings and suggest remediation steps.

Chapter 6: Post-Exploitation and Privilege Escalation – Maintaining and Expanding Access

After gaining initial access, the tester may attempt to maintain access and escalate privileges:

Maintaining Access: This involves establishing persistent access to the compromised system, which might involve installing backdoors or exploiting other vulnerabilities.
Gaining Higher Privileges: This involves obtaining higher-level access rights, such as administrator or root access, allowing the tester to access more sensitive information and system resources.
Lateral Movement: This involves moving from one compromised system to other systems within the network, expanding the scope of the attack.

Post-exploitation and privilege escalation are advanced techniques that require significant skill and knowledge.

Chapter 7: Security Hardening and Mitigation – Strengthening Defenses

This chapter covers implementing security best practices to mitigate identified vulnerabilities:

Implementing Security Best Practices: This includes implementing strong passwords, enabling firewalls, regularly updating software, and employing multi-factor authentication.
Patching Vulnerabilities: This involves installing security patches to address known vulnerabilities.
Intrusion Detection Systems (IDS): These systems monitor network traffic for suspicious activity and alert administrators to potential security breaches.

Conclusion: The Ongoing Evolution of Cybersecurity

This guide has covered the fundamental concepts of hacking and penetration testing. Remember, ethical hacking is a critical component of a robust cybersecurity strategy. The ever-evolving threat landscape demands continuous learning and adaptation. Stay updated on the latest vulnerabilities, techniques, and best practices to maintain a strong security posture.

FAQs

1. Is penetration testing legal? Yes, when performed with proper authorization. Unauthorized penetration testing is illegal and carries serious consequences.
2. What are the ethical considerations of penetration testing? Testers must respect the confidentiality, integrity, and availability of the target system. They must only access systems with explicit permission.
3. What are some popular penetration testing tools? Nmap, Metasploit, Burp Suite, Wireshark, Nessus.
4. What is the difference between a black box and white box penetration test? Black box tests simulate real-world attacks with no prior knowledge, while white box tests leverage full system knowledge.
5. How can I learn more about penetration testing? Take online courses, read books and articles, and practice in a controlled environment (e.g., a virtual machine).
6. What certifications are available for penetration testers? CompTIA Security+, CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional).
7. What are the career prospects for penetration testers? High demand and competitive salaries in the cybersecurity industry.
8. Is programming necessary for penetration testing? While not strictly required for all aspects, strong programming skills are beneficial for advanced techniques and exploit development.
9. What is the importance of reporting in penetration testing? Detailed reports document findings, prioritize vulnerabilities, and provide actionable recommendations for remediation.

Related Articles:

1. Ethical Hacking vs. Penetration Testing: Key Differences: This article clarifies the subtle distinctions between the two terms and highlights the ethical considerations.
2. Top 10 Penetration Testing Tools for Beginners: A curated list of user-friendly tools suitable for beginners in the field.
3. A Beginner's Guide to Network Security: This article lays the groundwork for understanding network security principles and concepts.
4. Understanding Common Web Application Vulnerabilities: A detailed explanation of common web vulnerabilities like SQL injection and XSS.
5. How to Build a Home Penetration Testing Lab: A step-by-step guide on setting up a safe and legal

practice environment.
6. The Importance of Vulnerability Scanning in Cybersecurity: This article emphasizes the role of vulnerability scanning in proactive security.
7. Social Engineering Techniques Used in Penetration Testing: A deep dive into the psychology and tactics behind social engineering.
8. Mastering Privilege Escalation Techniques: An advanced guide to gaining higher-level access in a compromised system.
9. Penetration Testing Report Writing Best Practices: This article covers the essential elements of a comprehensive and effective penetration testing report.

the basics of hacking and penetration testing 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

the basics of hacking and penetration testing 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.

the basics of hacking and penetration testing pdf: Ethical Hacking and Penetration Testing Guide Rafay Baloch, 2017-09-29 Requiring no prior hacking experience, Ethical Hacking and Penetration Testing Guide supplies a complete introduction to the steps required to complete a penetration test, or ethical hack, from beginning to end. You will learn how to properly utilize and interpret the results of modern-day hacking tools, which are required to complete a penetration test.

The book covers a wide range of tools, including Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. Supplying a simple and clean explanation of how to effectively utilize these tools, it details a four-step methodology for conducting an effective penetration test or hack.Providing an accessible introduction to penetration testing and hacking, the book supplies you with a fundamental understanding of offensive security. After completing the book you will be prepared to take on in-depth and advanced topics in hacking and penetration testing. The book walks you through each of the steps and tools in a structured, orderly manner allowing you to understand how the output from each tool can be fully utilized in the subsequent phases of the penetration test. This process will allow you to clearly see how the various tools and phases relate to each other. An ideal resource for those who want to learn about ethical hacking but don't know where to start, this book will help take your hacking skills to the next level. The topics described in this book comply with international standards and with what is being taught in international certifications.

the basics of hacking and penetration testing pdf: The Basics of Hacking and Penetration Testing Patrick Engebretson, 2011 The Basics of Hacking and Penetration Testing serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. This book makes ethical hacking and penetration testing easy - no prior hacking experience is required. It shows how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. With a simple and clean explanation of how to effectively utilize these tools - as well as the introduction to a four-step methodology for conducting a penetration test or hack - the book provides students with the know-how required to jump start their careers and gain a better understanding of offensive security. The book is organized into 7 chapters that cover hacking tools such as Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. PowerPoint slides are available for use in class. This book is an ideal reference for security consultants, beginning InfoSec professionals, and students. Named a 2011 Best Hacking and Pen Testing Book by InfoSec Reviews Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Writen by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Backtrack Linus distribution and focuses on the seminal tools required to complete a penetration test.

the basics of hacking and penetration testing 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

the basics of hacking and penetration testing pdf: Professional Penetration Testing Thomas Wilhelm, 2013-06-27 Professional Penetration Testing walks you through the entire process of setting up and running a pen test lab. Penetration testing—the act of testing a computer network to find security vulnerabilities before they are maliciously exploited—is a crucial component of information security in any organization. With this book, you will find out how to turn hacking skills into a professional career. Chapters cover planning, metrics, and methodologies; the details of running a pen test, including identifying and verifying vulnerabilities; and archiving, reporting and management practices. Author Thomas Wilhelm has delivered penetration testing training to countless security professionals, and now through the pages of this book you can benefit from his years of experience as a professional penetration tester and educator. After reading this book, you will be able to create a personal penetration test lab that can deal with real-world vulnerability scenarios. All disc-based content for this title is now available on the Web. - Find out how to turn hacking and pen testing skills into a professional career - Understand how to conduct controlled attacks on a network through real-world examples of vulnerable and exploitable servers - Master project management skills necessary for running a formal penetration test and setting up a professional ethical hacking business - Discover metrics and reporting methodologies that provide experience crucial to a professional penetration tester

the basics of hacking and penetration testing 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.

the basics of hacking and penetration testing 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.

the basics of hacking and penetration testing 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

the basics of hacking and penetration testing pdf: The Basics of Hacking and Penetration Testing Patrick Engebretson, 2011-07-21 The Basics of Hacking and Penetration Testing serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. This book makes ethical hacking and penetration testing easy – no prior hacking experience is required. It shows how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. With a simple and clean explanation of how to effectively utilize these tools – as well as the introduction to a four-step methodology for conducting a penetration test or hack – the book provides students with the know-how required to jump start their careers and gain a better understanding of offensive security. The book is organized into 7 chapters that cover hacking tools such as Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. PowerPoint slides are available for use in class. This book is an ideal reference for security consultants, beginning InfoSec professionals, and students. - Named a 2011 Best Hacking and Pen Testing Book by InfoSec Reviews - Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. - Writen by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. - Utilizes the Backtrack Linus distribution and focuses on the seminal tools required to complete a penetration test.

the basics of hacking and penetration testing 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?

the basics of hacking and penetration testing 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.

the basics of hacking and penetration testing pdf: From Hacking to Report Writing Robert Svensson, 2016-11-04 Learn everything you need to know to become a professional security and penetration tester. It simplifies hands-on security and penetration testing by breaking down each step of the process so that finding vulnerabilities and misconfigurations becomes easy. The book explains how to methodically locate, exploit, and professionally report security weaknesses using techniques such as SQL-injection, denial-of-service attacks, and password hacking. Although From Hacking to Report Writing will give you the technical know-how needed to carry out advanced security tests, it also offers insight into crafting professional looking reports describing your work and how your customers can benefit from it. The book will give you the tools you need to clearly communicate the benefits of high-quality security and penetration testing to IT-management, executives and other stakeholders. Embedded in the book are a number of on-the-job stories that will give you a good understanding of how you can apply what you have learned to real-world situations. We live in a time where computer security is more important than ever. Staying one step ahead of hackers has never been a bigger challenge. From Hacking to Report Writing clarifies how you can sleep better at night knowing that your network has been thoroughly tested. What you'll learn Clearly understand why security and penetration testing is important Find vulnerabilities in any system using the same techniques as hackers do Write professional looking reports Know which security and penetration testing method to apply for any given situation Successfully hold together a security and penetration test project Who This Book Is For Aspiring security and penetration testers, security consultants, security and penetration testers, IT managers, and security researchers.

the basics of hacking and penetration testing 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.

the basics of hacking and penetration testing pdf: *The Art of Network Penetration Testing* Royce Davis, 2020-12-29 The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. Summary Penetration testing is about more than just getting through a perimeter firewall. The biggest security threats are inside the network, where attackers can rampage through sensitive data by exploiting weak access controls and poorly patched software. Designed for up-and-coming security professionals, The Art of Network Penetration Testing teaches you how to take over an enterprise network from the inside. It lays out every stage of an internal security assessment step-by-step, showing you how to identify weaknesses before a malicious invader can do real damage. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Penetration testers uncover security gaps by attacking networks exactly like malicious intruders do. To become a world-class pentester, you need to master offensive security concepts, leverage a proven methodology, and practice, practice, practice. Th is book delivers insights from security expert Royce Davis, along with a virtual testing environment you can use to hone your skills. About the book The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. As you brute force passwords, exploit unpatched services, and elevate network level privileges, you'll learn where the weaknesses are—and how to take advantage of them. What's inside Set up a virtual pentest lab Exploit Windows and Linux network vulnerabilities Establish persistent re-entry to compromised targets Detail your findings in an engagement report About the reader For tech professionals. No security experience required. About the author Royce Davis has orchestrated hundreds of penetration tests, helping to secure many of the largest companies in the world. Table of Contents 1 Network Penetration Testing PHASE 1 - INFORMATION GATHERING 2 Discovering network hosts 3 Discovering network services 4 Discovering network vulnerabilities PHASE 2 - FOCUSED PENETRATION 5 Attacking vulnerable web services 6 Attacking vulnerable database services 7 Attacking unpatched services PHASE 3 - POST-EXPLOITATION AND PRIVILEGE ESCALATION 8 Windows post-exploitation 9 Linux or UNIX post-exploitation 10 Controlling the entire network PHASE 4 - DOCUMENTATION 11 Post-engagement cleanup 12 Writing a solid

pentest deliverable

the basics of hacking and penetration testing pdf: Building Virtual Pentesting Labs for Advanced Penetration Testing Kevin Cardwell, 2016-08-30 Learn how to build complex virtual architectures that allow you to perform virtually any required testing methodology and perfect it About This Book Explore and build intricate architectures that allow you to emulate an enterprise network Test and enhance your security skills against complex and hardened virtual architecture Learn methods to bypass common enterprise defenses and leverage them to test the most secure environments. Who This Book Is For While the book targets advanced penetration testing, the process is systematic and as such will provide even beginners with a solid methodology and approach to testing. You are expected to have network and security knowledge. The book is intended for anyone who wants to build and enhance their existing professional security and penetration testing methods and skills. What You Will Learn Learning proven security testing and penetration testing techniques Building multi-layered complex architectures to test the latest network designs Applying a professional testing methodology Determining whether there are filters between you and the target and how to penetrate them Deploying and finding weaknesses in common firewall architectures. Learning advanced techniques to deploy against hardened environments Learning methods to circumvent endpoint protection controls In Detail Security flaws and new hacking techniques emerge overnight – security professionals need to make sure they always have a way to keep . With this practical guide, learn how to build your own virtual pentesting lab environments to practice and develop your security skills. Create challenging environments to test your abilities, and overcome them with proven processes and methodologies used by global penetration testing teams. Get to grips with the techniques needed to build complete virtual machines perfect for pentest training. Construct and attack layered architectures, and plan specific attacks based on the platforms you're going up against. Find new vulnerabilities for different kinds of systems and networks, and what these mean for your clients. Driven by a proven penetration testing methodology that has trained thousands of testers, Building Virtual Labs for Advanced Penetration Testing, Second Edition will prepare you for participation in professional security teams. Style and approach The book is written in an easy-to-follow format that provides a step–by-step, process-centric approach. Additionally, there are numerous hands-on examples and additional references for readers who might want to learn even more. The process developed throughout the book has been used to train and build teams all around the world as professional security and penetration testers.

the basics of hacking and penetration testing 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.

the basics of hacking and penetration testing 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.

the basics of hacking and penetration testing pdf: Quick Start Guide to Penetration Testing Sagar Rahalkar, 2018-11-29 Get started with NMAP, OpenVAS, and Metasploit in this short book and understand how NMAP, OpenVAS, and Metasploit can be integrated with each other for greater flexibility and efficiency. You will begin by working with NMAP and ZENMAP and learning the basic scanning and enumeration process. After getting to know the differences between TCP and UDP scans, you will learn to fine tune your scans and efficiently use NMAP scripts. This will be followed by an introduction to OpenVAS vulnerability management system. You will then learn to configure OpenVAS and scan for and report vulnerabilities. The next chapter takes you on a detailed tour of Metasploit and its basic commands and configuration. You will then invoke NMAP and OpenVAS scans from Metasploit. Lastly, you will take a look at scanning services with Metasploit and get to know more about Meterpreter, an advanced, dynamically extensible payload that is extended over the network at runtime. The final part of the book concludes by pentesting a system in a real-world scenario, where you will apply the skills you have learnt. What You Will Learn Carry out basic scanning with NMAPInvoke NMAP from Python Use vulnerability scanning and reporting with OpenVAS Master common commands in Metasploit Who This Book Is For Readers new to penetration testing who would like to get a quick start on it.

the basics of hacking and penetration testing pdf: Metasploit David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, 2011-07-15 The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester's Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors. Once you've built your foundation for penetration testing, you'll learn the Framework's conventions, interfaces, and module system as you launch simulated attacks. You'll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks. Learn how to: –Find and exploit unmaintained, misconfigured, and unpatched systems –Perform reconnaissance and find valuable information about your target –Bypass anti-virus technologies and circumvent security controls –Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery –Use the Meterpreter shell to launch further attacks from inside the network –Harness standalone Metasploit utilities, third-party tools, and plug-ins –Learn how to write your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework,

and learn how to cover your tracks. Whether your goal is to secure your own networks or to put someone else's to the test, Metasploit: The Penetration Tester's Guide will take you there and beyond.

the basics of hacking and penetration testing 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

the basics of hacking and penetration testing 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.

the basics of hacking and penetration testing pdf: *Hands on Hacking* Matthew Hickey, Jennifer Arcuri, 2020-09-16 A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking techniques to better understand real-world risks to computer networks and data. Readers will benefit from the

author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker’s perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you’ll look for flaws and their known exploits—including tools developed by real-world government financed state-actors. An introduction to the same hacking techniques that malicious hackers will use against an organization Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws Based on the tried and tested material used to train hackers all over the world in the art of breaching networks Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won't find any hypothetical academic only attacks here. From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to advanced techniques in a structured learning format.

the basics of hacking and penetration testing 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.

the basics of hacking and penetration testing pdf: *Learn Penetration Testing* Rishalin Pillay, 2019-05-31 Get up to speed with various penetration testing techniques and resolve security threats of varying complexity Key FeaturesEnhance your penetration testing skills to tackle security threatsLearn to gather information, find vulnerabilities, and exploit enterprise defensesNavigate secured systems with the most up-to-date version of Kali Linux (2019.1) and Metasploit (5.0.0)Book Description Sending information via the internet is not entirely private, as evidenced by the rise in hacking, malware attacks, and security threats. With the help of this book, you'll learn crucial penetration testing techniques to help you evaluate enterprise defenses. You'll start by understanding each stage of pentesting and deploying target virtual machines, including Linux and

Windows. Next, the book will guide you through performing intermediate penetration testing in a controlled environment. With the help of practical use cases, you'll also be able to implement your learning in real-world scenarios. By studying everything from setting up your lab, information gathering and password attacks, through to social engineering and post exploitation, you'll be able to successfully overcome security threats. The book will even help you leverage the best tools, such as Kali Linux, Metasploit, Burp Suite, and other open source pentesting tools to perform these techniques. Toward the later chapters, you'll focus on best practices to quickly resolve security threats. By the end of this book, you'll be well versed with various penetration testing techniques so as to be able to tackle security threats effectively What you will learnPerform entry-level penetration tests by learning various concepts and techniquesUnderstand both common and not-so-common vulnerabilities from an attacker's perspectiveGet familiar with intermediate attack methods that can be used in real-world scenariosUnderstand how vulnerabilities are created by developers and how to fix some of them at source code levelBecome well versed with basic tools for ethical hacking purposesExploit known vulnerable services with tools such as MetasploitWho this book is for If you’re just getting started with penetration testing and want to explore various security domains, this book is for you. Security professionals, network engineers, and amateur ethical hackers will also find this book useful. Prior knowledge of penetration testing and ethical hacking is not necessary.

the basics of hacking and penetration testing pdf: Penetration Testing Fundamentals William Easttom II, 2018-03-06 The perfect introduction to pen testing for all IT professionals and students · Clearly explains key concepts, terminology, challenges, tools, and skills · Covers the latest penetration testing standards from NSA, PCI, and NIST Welcome to today’s most useful and practical introduction to penetration testing. Chuck Easttom brings together up-to-the-minute coverage of all the concepts, terminology, challenges, and skills you’ll need to be effective. Drawing on decades of experience in cybersecurity and related IT fields, Easttom integrates theory and practice, covering the entire penetration testing life cycle from planning to reporting. You’ll gain practical experience through a start-to-finish sample project relying on free open source tools. Throughout, quizzes, projects, and review sections deepen your understanding and help you apply what you’ve learned. Including essential pen testing standards from NSA, PCI, and NIST, Penetration Testing Fundamentals will help you protect your assets–and expand your career options. LEARN HOW TO · Understand what pen testing is and how it’s used · Meet modern standards for comprehensive and effective testing · Review cryptography essentials every pen tester must know · Perform reconnaissance with Nmap, Google searches, and ShodanHq · Use malware as part of your pen testing toolkit · Test for vulnerabilities in Windows shares, scripts, WMI, and the Registry · Pen test websites and web communication · Recognize SQL injection and cross-site scripting attacks · Scan for vulnerabilities with OWASP ZAP, Vega, Nessus, and MBSA · Identify Linux vulnerabilities and password cracks · Use Kali Linux for advanced pen testing · Apply general hacking technique ssuch as fake Wi-Fi hotspots and social engineering · Systematically test your environment with Metasploit · Write or customize sophisticated Metasploit exploits

the basics of hacking and penetration testing pdf: *Practical Web Penetration Testing* Gus Khawaja, 2018-06-22 Web Applications are the core of any business today, and the need for specialized Application Security experts is increasing these days. Using this book, you will be able to learn Application Security testing and understand how to analyze a web application, conduct a web intrusion test, and a network infrastructure test.

the basics of hacking and penetration testing 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!

the basics of hacking and penetration testing pdf: Penetration Tester's Open Source Toolkit Jeremy Faircloth, 2011-08-25 Penetration Tester's Open Source Toolkit, Third Edition, discusses the open source tools available to penetration testers, the ways to use them, and the situations in which they apply. Great commercial penetration testing tools can be very expensive and sometimes hard to use or of questionable accuracy. This book helps solve both of these problems. The open source, no-cost penetration testing tools presented do a great job and can be modified by the student for each situation. This edition offers instruction on how and in which situations the penetration tester can best use them. Real-life scenarios support and expand upon explanations throughout. It also presents core technologies for each type of testing and the best tools for the job. The book consists of 10 chapters that covers a wide range of topics such as reconnaissance; scanning and enumeration; client-side attacks and human weaknesses; hacking database services; Web server and Web application testing; enterprise application testing; wireless penetrating testing; and building penetration test labs. The chapters also include case studies where the tools that are discussed are applied. New to this edition: enterprise application testing, client-side attacks and updates on Metasploit and Backtrack. This book is for people who are interested in penetration testing or professionals engaged in penetration testing. Those working in the areas of database, network, system, or application administration, as well as architects, can gain insights into how penetration testers perform testing in their specific areas of expertise and learn what to expect from a penetration test. This book can also serve as a reference for security or audit professionals. - Details current open source penetration testing tools - Presents core technologies for each type of testing and the best tools for the job - New to this edition: Enterprise application testing, client-side attacks and updates on Metasploit and Backtrack

the basics of hacking and penetration testing pdf: *Google Hacking for Penetration Testers* Johnny Long, 2004-12-17 Google, the most popular search engine worldwide, provides web surfers with an easy-to-use guide to the Internet, with web and image searches, language translation, and a range of features that make web navigation simple enough for even the novice user. What many users don't realize is that the deceptively simple components that make Google so easy to use are the same features that generously unlock security flaws for the malicious hacker. Vulnerabilities in website security can be discovered through Google hacking, techniques applied to the search engine by computer criminals, identity thieves, and even terrorists to uncover secure information. This book beats Google hackers to the punch, equipping web administrators with penetration testing applications to ensure their site is invulnerable to a hacker's search. Penetration Testing with Google Hacks explores the explosive growth of a technique known as Google Hacking. When the modern security landscape includes such heady topics as blind SQL injection and integer overflows, it's refreshing to see such a deceptively simple tool bent to achieve such amazing results; this is hacking in the purest sense of the word. Readers will learn how to torque Google to detect SQL injection points and login portals, execute port scans and CGI scans, fingerprint web servers, locate incredible information caches such as firewall and IDS logs, password databases, SQL dumps and

much more - all without sending a single packet to the target! Borrowing the techniques pioneered by malicious Google hackers, this talk aims to show security practitioners how to properly protect clients from this often overlooked and dangerous form of information leakage.*First book about Google targeting IT professionals and security leaks through web browsing. *Author Johnny Long, the authority on Google hacking, will be speaking about Google Hacking at the Black Hat 2004 Briefing. His presentation on penetrating security flaws with Google is expected to create a lot of buzz and exposure for the topic. *Johnny Long's Web site hosts the largest repository of Google security exposures and is the most popular destination for security professionals who want to learn about the dark side of Google.

the basics of hacking and penetration testing pdf: The Car Hacker's Handbook Craig Smith, 2016-03-01 Modern cars are more computerized than ever. Infotainment and navigation systems, Wi-Fi, automatic software updates, and other innovations aim to make driving more convenient. But vehicle technologies haven’t kept pace with today’s more hostile security environment, leaving millions vulnerable to attack. The Car Hacker’s Handbook will give you a deeper understanding of the computer systems and embedded software in modern vehicles. It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and between devices and systems. Then, once you have an understanding of a vehicle’s communication network, you’ll learn how to intercept data and perform specific hacks to track vehicles, unlock doors, glitch engines, flood communication, and more. With a focus on low-cost, open source hacking tools such as Metasploit, Wireshark, Kayak, can-utils, and ChipWhisperer, The Car Hacker’s Handbook will show you how to: –Build an accurate threat model for your vehicle –Reverse engineer the CAN bus to fake engine signals –Exploit vulnerabilities in diagnostic and data-logging systems –Hack the ECU and other firmware and embedded systems –Feed exploits through infotainment and vehicle-to-vehicle communication systems –Override factory settings with performance-tuning techniques –Build physical and virtual test benches to try out exploits safely If you’re curious about automotive security and have the urge to hack a two-ton computer, make The Car Hacker’s Handbook your first stop.

the basics of hacking and penetration testing pdf: Mastering Modern Web Penetration Testing Prakhar Prasad, 2016-10-28 Master the art of conducting modern pen testing attacks and techniques on your web application before the hacker does! About This Book This book covers the latest technologies such as Advance XSS, XSRF, SQL Injection, Web API testing, XML attack vectors, OAuth 2.0 Security, and more involved in today's web applications Penetrate and secure your web application using various techniques Get this comprehensive reference guide that provides advanced tricks and tools of the trade for seasoned penetration testers Who This Book Is For This book is for security professionals and penetration testers who want to speed up their modern web application penetrating testing. It will also benefit those at an intermediate level and web developers who need to be aware of the latest application hacking techniques. What You Will Learn Get to know the new and less-publicized techniques such PHP Object Injection and XML-based vectors Work with different security tools to automate most of the redundant tasks See different kinds of newly-designed security headers and how they help to provide security Exploit and detect different kinds of XSS vulnerabilities Protect your web application using filtering mechanisms Understand old school and classic web hacking in depth using SQL Injection, XSS, and CSRF Grasp XML-related vulnerabilities and attack vectors such as XXE and DoS techniques Get to know how to test REST APIs to discover security issues in them In Detail Web penetration testing is a growing, fast-moving, and absolutely critical field in information security. This book executes modern web application attacks and utilises cutting-edge hacking techniques with an enhanced knowledge of web application security. We will cover web hacking techniques so you can explore the attack vectors during penetration tests. The book encompasses the latest technologies such as OAuth 2.0, Web API testing methodologies and XML vectors used by hackers. Some lesser discussed attack vectors such as RPO (relative path overwrite), DOM clobbering, PHP Object Injection and etc. has been covered in this book. We'll explain various old school techniques in depth such as XSS, CSRF, SQL Injection through

the ever-dependable SQLMap and reconnaissance. Websites nowadays provide APIs to allow integration with third party applications, thereby exposing a lot of attack surface, we cover testing of these APIs using real-life examples. This pragmatic guide will be a great benefit and will help you prepare fully secure applications. Style and approach This master-level guide covers various techniques serially. It is power-packed with real-world examples that focus more on the practical aspects of implementing the techniques rather going into detailed theory.

the basics of hacking and penetration testing pdf: Ethical Hacking Daniel G. Graham, 2021-09-21 A hands-on guide to hacking computer systems from the ground up, from capturing traffic to crafting sneaky, successful trojans. A crash course in modern hacking techniques, Ethical Hacking is already being used to prepare the next generation of offensive security experts. In its many hands-on labs, you'll explore crucial skills for any aspiring penetration tester, security researcher, or malware analyst. You'll begin with the basics: capturing a victim's network traffic with an ARP spoofing attack and then viewing it in Wireshark. From there, you'll deploy reverse shells that let you remotely run commands on a victim's computer, encrypt files by writing your own ransomware in Python, and fake emails like the ones used in phishing attacks. In advanced chapters, you'll learn how to fuzz for new vulnerabilities, craft trojans and rootkits, exploit websites with SQL injection, and escalate your privileges to extract credentials, which you'll use to traverse a private network. You'll work with a wide range of professional penetration testing tools—and learn to write your own tools in Python—as you practice tasks like: • Deploying the Metasploit framework's reverse shells and embedding them in innocent-seeming files • Capturing passwords in a corporate Windows network using Mimikatz • Scanning (almost) every device on the internet to find potential victims • Installing Linux rootkits that modify a victim's operating system • Performing advanced Cross-Site Scripting (XSS) attacks that execute sophisticated JavaScript payloads Along the way, you'll gain a foundation in the relevant computing technologies. Discover how advanced fuzzers work behind the scenes, learn how internet traffic gets encrypted, explore the inner mechanisms of nation-state malware like Drovorub, and much more. Developed with feedback from cybersecurity students, Ethical Hacking addresses contemporary issues in the field not often covered in other books and will prepare you for a career in penetration testing. Most importantly, you'll be able to think like an ethical hacker: someone who can carefully analyze systems and creatively gain access to them.

the basics of hacking and penetration testing pdf: Backtrack 5 Wireless Penetration Testing Vivek Ramachandran, 2011-09-09 Wireless has become ubiquitous in today's world. The mobility and flexibility provided by it makes our lives more comfortable and productive. But this comes at a cost – Wireless technologies are inherently insecure and can be easily broken. BackTrack is a penetration testing and security auditing distribution that comes with a myriad of wireless networking tools used to simulate network attacks and detect security loopholes. Backtrack 5 Wireless Penetration Testing Beginner's Guide will take you through the journey of becoming a Wireless hacker. You will learn various wireless testing methodologies taught using live examples, which you will implement throughout this book. The engaging practical sessions very gradually grow in complexity giving you enough time to ramp up before you get to advanced wireless attacks. This book will take you through the basic concepts in Wireless and creating a lab environment for your experiments to the business of different lab sessions in wireless security basics, slowly turn on the heat and move to more complicated scenarios, and finally end your journey by conducting bleeding edge wireless attacks in your lab. There are many interesting and new things that you will learn in this book – War Driving, WLAN packet sniffing, Network Scanning, Circumventing hidden SSIDs and MAC filters, bypassing Shared Authentication, Cracking WEP and WPA/WPA2 encryption, Access Point MAC spoofing, Rogue Devices, Evil Twins, Denial of Service attacks, Viral SSIDs, Honeypot and Hotspot attacks, Caffe Latte WEP Attack, Man-in-the-Middle attacks, Evading Wireless Intrusion Prevention systems and a bunch of other cutting edge wireless attacks. If you were ever curious about what wireless security and hacking was all about, then this book will get you started by providing you with the knowledge and practical know-how to become a wireless hacker. Hands-on

practical guide with a step-by-step approach to help you get started immediately with Wireless Penetration Testing

the basics of hacking and penetration testing pdf: Bug Bounty Hunting Essentials Carlos A. Lozano, Shahmeer Amir, 2018-11-30 Get hands-on experience on concepts of Bug Bounty Hunting Key FeaturesGet well-versed with the fundamentals of Bug Bounty HuntingHands-on experience on using different tools for bug huntingLearn to write a bug bounty report according to the different vulnerabilities and its analysisBook Description Bug bounty programs are the deals offered by prominent companies where-in any white-hat hacker can find bugs in the applications and they will have a recognition for the same. The number of prominent organizations having this program has increased gradually leading to a lot of opportunity for Ethical Hackers. This book will initially start with introducing you to the concept of Bug Bounty hunting. Then we will dig deeper into concepts of vulnerabilities and analysis such as HTML injection, CRLF injection and so on. Towards the end of the book, we will get hands-on experience working with different tools used for bug hunting and various blogs and communities to be followed. This book will get you started with bug bounty hunting and its fundamentals. What you will learnLearn the basics of bug bounty huntingHunt bugs in web applicationsHunt bugs in Android applicationsAnalyze the top 300 bug reportsDiscover bug bounty hunting research methodologiesExplore different tools used for Bug HuntingWho this book is for This book is targeted towards white-hat hackers, or anyone who wants to understand the concept behind bug bounty hunting and understand this brilliant way of penetration testing. This book does not require any knowledge on bug bounty hunting.

the basics of hacking and penetration testing pdf: Penetration Testing Bootcamp Jason Beltrame, 2017-06-28 Sharpen your pentesting skill in a bootcamp About This Book Get practical demonstrations with in-depth explanations of complex security-related problems Familiarize yourself with the most common web vulnerabilities Get step-by-step guidance on managing testing results and reporting Who This Book Is For This book is for IT security enthusiasts and administrators who want to understand penetration testing quickly. What You Will Learn Perform different attacks such as MiTM, and bypassing SSL encryption 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 Recover lost files, investigate successful hacks, and discover hidden data Write organized and effective penetration testing reports In Detail Penetration Testing Bootcamp delivers practical, learning modules in manageable chunks. Each chapter is delivered in a day, and each day builds your competency in Penetration Testing. This book will begin by taking you through the basics and show you how to set up and maintain the C&C Server. You will also understand how to scan for vulnerabilities and Metasploit, learn how to setup connectivity to a C&C server and maintain that connectivity for your intelligence gathering as well as offsite processing. Using TCPDump filters, you will gain understanding of the sniffing and spoofing traffic. This book will also teach you the importance of clearing up the tracks you leave behind after the penetration test and will show you how to build a report from all the data obtained from the penetration test. In totality, this book will equip you with instructions through rigorous tasks, practical callouts, and assignments to reinforce your understanding of penetration testing. Style and approach This book is delivered in the form of a 10-day boot camp style book. The day-by-day approach will help you get to know everything about penetration testing, from the use of network reconnaissance tools, to the writing of custom zero-day buffer overflow exploits.

the basics of hacking and penetration testing 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.

the basics of hacking and penetration testing pdf: Mastering Kali Linux for Advanced Penetration Testing Robert W. Beggs, 2014-06-24 This book provides an overview of the kill chain approach to penetration testing, and then focuses on using Kali Linux to provide examples of how this methodology is applied in the real world. After describing the underlying concepts, step-by-step examples are provided that use selected tools to demonstrate the techniques.If you are an IT professional or a security consultant who wants to maximize the success of your network testing using some of the advanced features of Kali Linux, then this book is for you. This book will teach you how to become an expert in the pre-engagement, management, and documentation of penetration testing by building on your understanding of Kali Linux and wireless concepts.

the basics of hacking and penetration testing pdf: Hacker Techniques, Tools, and Incident Handling Sean-Philip Oriyano, Michael G. Solomon, 2018-09-04 Hacker Techniques, Tools, and Incident Handling, Third Edition begins with an examination of the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals who break into networks, steal information, and corrupt data. It goes on to review the technical overview of hacking: how attacks target networks and the methodology they follow. The final section studies those methods that are most effective when dealing with hacking attacks, especially in an age of increased reliance on the Web. Written by subject matter experts, with numerous real-world examples, Hacker Techniques, Tools, and Incident Handling, Third Edition provides readers with a clear, comprehensive introduction to the many threats on our Internet environment and security and what can be done to combat them.

the basics of hacking and penetration testing pdf: Practical Hardware Pentesting Jean-Georges Valle, 2021-04-01 Learn how to pentest your hardware with the most common attract techniques and patterns Key FeaturesExplore various pentesting tools and techniques to secure your hardware infrastructureProtect your hardware by finding potential entry points like glitchesFind the best practices for securely designing your productsBook Description If you're looking for hands-on introduction to pentesting that delivers, then Practical Hardware Pentesting is for you. This book will help you plan attacks, hack your embedded devices, and secure the hardware infrastructure. Throughout the book, you will see how a specific device works, explore the functional and security aspects, and learn how a system senses and communicates with the outside world. You'll set up a lab from scratch and then gradually work towards an advanced hardware lab—but you'll still be able to follow along with a basic setup. As you progress, you'll get to grips with the global architecture of an embedded system and sniff on-board traffic, learn how to identify and formalize threats to the

embedded system, and understand its relationship with its ecosystem. You'll discover how to analyze your hardware and locate its possible system vulnerabilities before going on to explore firmware dumping, analysis, and exploitation. The reverse engineering chapter will get you thinking from an attacker point of view; you'll understand how devices are attacked, how they are compromised, and how you can harden a device against the most common hardware attack vectors. By the end of this book, you will be well-versed with security best practices and understand how they can be implemented to secure your hardware. What you will learnPerform an embedded system test and identify security critical functionalitiesLocate critical security components and buses and learn how to attack them Discover how to dump and modify stored informationUnderstand and exploit the relationship between the firmware and hardwareIdentify and attack the security functions supported by the functional blocks of the deviceDevelop an attack lab to support advanced device analysis and attacksWho this book is for If you're a researcher or a security professional who wants a comprehensive introduction into hardware security assessment, then this book is for you. Electrical engineers who want to understand the vulnerabilities of their devices and design them with security in mind will also find this book useful. You won't need any prior knowledge with hardware pentensting before you get started; everything you need is in the chapters.

Related Articles

- the bible for dummies pdf
- taoist tai chi moves step by step
- the benefits of trade mastery test

Back to Home