

Advanced Penetration Testing Hacking The Worlds Most Secure Networks

This book helps people find sensitive information on the Web. Google is one of the 5 most popular sites on the internet with more than 380 million unique users per month (Nielsen/NetRatings 8/05). But, Google's search capabilities are so powerful, they sometimes discover content that no one ever intended to be publicly available on the Web including: social security numbers, credit card numbers, trade secrets, and federally classified documents. Google Hacking for Penetration Testers Volume 2 shows the art of manipulating Google used by security professionals and system administrators to find this sensitive information and "self-police their own organizations. Readers will learn how Google Maps and Google Earth provide pinpoint military accuracy, see how bad guys can manipulate Google to create super worms, and see how they can "mash up" Google with MySpace, LinkedIn, and more for passive reconnaissance. • Learn Google Searching Basics Explore Google's Web-based Interface, build Google queries, and work with Google URLs. • Use Advanced Operators to Perform Advanced Queries Combine advanced operators and learn about colliding operators and bad search-fu. • Learn the Ways of the Google Hacker See how to use caches for anonymity and review directory listings and traversal techniques. • Review Document Grinding and Database Digging See the ways to use Google to locate documents and then search within the documents to locate information. • Understand Google's Part in an Information Collection Framework Learn the principles of automating searches and the applications of data mining. • Locate Exploits and Finding Targets Locate exploit code and then vulnerable targets. • See Ten Simple Security Searches Learn a few searches that give good results just about every time and are good for a security assessment. • Track Down Web Servers Locate and profile web servers, login portals, network hardware and utilities. • See How Bad Guys Troll for Data Find ways to search for usernames, passwords, credit card numbers, social security numbers, and other juicy information. • Hack Google Services Learn more about the AJAX Search API, Calendar, Blogger, Blog Search, and more.

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.

With more than 600 security tools in its arsenal, the Kali Linux distribution can be overwhelming. Experienced and aspiring security professionals alike may find it challenging to select the most appropriate tool for conducting a given test. This practical book covers Kali's expansive security capabilities and helps you identify the tools you need to conduct a wide range of security tests and penetration tests. You'll also explore the vulnerabilities that make those tests necessary. Author Ric Messier takes you through the foundations of Kali Linux and explains methods for conducting tests on networks, web applications, wireless security, password vulnerability, and more. You'll discover different techniques for extending Kali tools and creating your own toolset. Learn tools for stress testing network stacks and applications Perform network reconnaissance to determine what's available to attackers Execute penetration tests using automated exploit tools such as Metasploit Use cracking tools to see if passwords meet complexity requirements Test wireless capabilities by injecting frames and cracking passwords Assess web application vulnerabilities with automated or proxy-based tools Create advanced attack techniques by extending Kali tools or developing your own Use Kali Linux to generate reports once testing is complete

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?

This book delves deeper into analyzing the security of various AWS services and shows techniques and tactics used by an attacker to breach an AWS environment. This is the third part of the book series "Red Team: An attack paradigm".

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.

Advanced Penetration Testing Hacking the World's Most Secure Networks John Wiley & Sons

This is second edition of the book "Red Team: An Attack Paradigm". In the first edition, we had introduced the readers to Red Teaming concepts and focused on breaching the internal network of an organization. This book continues on the same theme and expands with new threat profiles that target different organizations. The books expands on techniques of privilege escalation and persistence both in Linux and Windows world. The book explores the new attack strategy that the organizations now need to embrace to combat the modern cyber threat. The book details from start to finish how to set up a Red Team practice within an organization. It defines the overall approach, the strategy required, the tools of the craft, etc. that would allow Information Security professionals within an organization to understand how they can set up a Red Team practice. The book also details the required infrastructure setup, defines examples of how to create engagements based on Threat Actor profiles and uses real world case studies as ways of justifying those examples. The book has been created with one goal in mind .i.e. to help security professionals use their current skill-sets and build on top of it to be a part of the new paradigm that will change the way organizations do their defense.

Hacker extraordinaire Kevin Mitnick delivers the explosive encore to his bestselling The Art of Deception Kevin Mitnick, the world's most celebrated hacker, now devotes his life to helping businesses and governments combat data thieves, cybervandals, and other malicious computer intruders. In his bestselling The Art of Deception, Mitnick presented fictionalized case studies that

illustrated how savvy computer crackers use "social engineering" to compromise even the most technically secure computer systems. Now, in his new book, Mitnick goes one step further, offering hair-raising stories of real-life computer break-ins-and showing how the victims could have prevented them. Mitnick's reputation within the hacker community gave him unique credibility with the perpetrators of these crimes, who freely shared their stories with him-and whose exploits Mitnick now reveals in detail for the first time, including: A group of friends who won nearly a million dollars in Las Vegas by reverse-engineering slot machines Two teenagers who were persuaded by terrorists to hack into the Lockheed Martin computer systems Two convicts who joined forces to become hackers inside a Texas prison A "Robin Hood" hacker who penetrated the computer systems of many prominent companies-and then told them how he gained access With riveting "you are there" descriptions of real computer break-ins, indispensable tips on countermeasures security professionals need to implement now, and Mitnick's own acerbic commentary on the crimes he describes, this book is sure to reach a wide audience-and attract the attention of both law enforcement agencies and the media.

HACKING - 5 BOOKS IN 1
BOOK 1: Beginners Guide
BOOK 2: Wireless Hacking
BOOK 3: 17 Most Tools Every Hacker Should Have
BOOK 4: 17 Most Dangerous Hacking Attacks
BOOK 5: 10 Most Dangerous Cyber Gangs
In this book you will learn about:
Basic Knowledge
The history of hacking, What motivates Hackers, and how to differentiate one to another
Networking fundamentals, and basic system requirements
Where to find the best operating systems for the purpose of Hacking
What virtualization is, and how to install Hacking software
Penetrating Wired Networks
Exploiting systems in multiple ways, Implementing Man in the Middle attack in multiple ways, How to use Social Engineering Toolkits, Creating a fake packet and find vulnerabilities, How to manipulate the network
Wireless Hacking
How to own a device connected remotely
How to find hidden wireless networks, How to implement a Rouge Wireless Access Point
Discovering networking devices through wireless
Exploiting systems in multiple ways using wireless technologies
Implementing Man in the Middle attack in multiple ways, How to become a wireless access point using your laptop
Hacking Attacks
ADVWARE - SPYWARE - MALWARE - MAN IN THE MIDDLE - LOCKY
TRAFFIC REDIRECTION - PAYLOAD INJECTION - ARP POISONING - WORMS
DE-AUTHENTICATION ATTACKS - COLLISION ATTACKS - REPLAY ATTACKS
PHISHING-VISHING - WHALING - SMISHING - SPEAR PHISHING
DUMPSTER DIVING - SHOULDER SURFING - BRUTE FORCE ATTACK - DICTIONARY ATTACKS
RAINBOW TABLES - KEYSTROKE LOGGINGS
SPOOFING - SOCIAL ENGINEERING-SPAMMING -SQL INJECTIONS - DDOS ATTACKS - TCP SYN FLOOD ATTACK
PING OF DEATH - VIRUSES ROOTKITS - LOGIC BOMBS - TROJAN HORSES
WANNAYCRY - RANSOMWARE - BOTNETS
CyberGangs
Cutting sword of justice, Guardians of Peace, Honker Union, Anonymous
Syrian Electronic Army, LulzSec, Carbanac, Equation Group, The Shadow Brokers

The first guide to planning and performing a physical penetration test on your computer's security
Most IT security teams concentrate on keeping networks and systems safe from attacks from the outside-but what if your attacker was on the inside?
While nearly all IT teams perform a variety of network and application penetration testing procedures, an audit and test of the

physical location has not been as prevalent. IT teams are now increasingly requesting physical penetration tests, but there is little available in terms of training. The goal of the test is to demonstrate any deficiencies in operating procedures concerning physical security. Featuring a Foreword written by world-renowned hacker Kevin D. Mitnick and lead author of *The Art of Intrusion* and *The Art of Deception*, this book is the first guide to planning and performing a physical penetration test. Inside, IT security expert Wil Allsopp guides you through the entire process from gathering intelligence, getting inside, dealing with threats, staying hidden (often in plain sight), and getting access to networks and data. Teaches IT security teams how to break into their own facility in order to defend against such attacks, which is often overlooked by IT security teams but is of critical importance Deals with intelligence gathering, such as getting access building blueprints and satellite imagery, hacking security cameras, planting bugs, and eavesdropping on security channels Includes safeguards for consultants paid to probe facilities unbeknown to staff Covers preparing the report and presenting it to management In order to defend data, you need to think like a thief-let Unauthorised Access show you how to get inside.

Written in an easy-to-follow approach using hands-on examples, this book helps you create virtual environments for advanced penetration testing, enabling you to build a multi-layered architecture to include firewalls, IDS/IPS, web application firewalls, and endpoint protection, which is essential in the penetration testing world.If you are a penetration tester, security consultant, security test engineer, or analyst who wants to practice and perfect penetration testing skills by building virtual pentesting labs in varying industry scenarios, this is the book for you. This book is ideal if you want to build and enhance your existing pentesting methods and skills. Basic knowledge of network security features is expected along with web application testing experience.

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

Learn how to execute web application penetration testing end-to-end Key Features Build an end-to-end threat model landscape for web application security Learn both web application vulnerabilities and web intrusion testing Associate network vulnerabilities with a web application infrastructure Book Description Companies all over the world want to hire professionals dedicated to application security. Practical Web Penetration Testing focuses on this very trend, teaching you how to conduct application security testing

using real-life scenarios. To start with, you'll set up an environment to perform web application penetration testing. You will then explore different penetration testing concepts such as threat modeling, intrusion test, infrastructure security threat, and more, in combination with advanced concepts such as Python scripting for automation. Once you are done learning the basics, you will discover end-to-end implementation of tools such as Metasploit, Burp Suite, and Kali Linux. Many companies deliver projects into production by using either Agile or Waterfall methodology. This book shows you how to assist any company with their SDLC approach and helps you on your journey to becoming an application security specialist. By the end of this book, you will have hands-on knowledge of using different tools for penetration testing. What you will learn

- Learn how to use Burp Suite effectively
- Use Nmap, Metasploit, and more tools for network infrastructure tests
- Practice using all web application hacking tools for intrusion tests using Kali Linux
- Learn how to analyze a web application using application threat modeling
- Know how to conduct web intrusion tests
- Understand how to execute network infrastructure tests
- Master automation of penetration testing functions for maximum efficiency using Python

Who this book is for: Practical Web Penetration Testing is for you if you are a security professional, penetration tester, or stakeholder who wants to execute penetration testing using the latest and most popular tools. Basic knowledge of ethical hacking would be an added advantage.

Are you interested in learning about how to hack systems? Do you want to learn how to protect yourself from being hacked? Do you wish to learn the art of ethical hacking? Do you want to know the secrets techniques that genius hackers use? Do you want to learn how to protect yourself from some of the most common hacking attacks? Hacking is one of the most misunderstood cyber concepts. The majority of people think of hacking as something evil or illegal, but nothing could be farther from the truth. Indeed, hacking can be a real threat, but if you want to stop someone from hacking you, you must also learn how to hack! In this book, "Hacking: The Ultimate Beginner-to-Expert Guide To Penetration Testing, Hacking, And Security Countermeasures," you will learn:

- The different types of hackers
- The different types of attacks
- The proven steps and techniques that the best hackers use
- Penetration testing
- Hacking Wi-Fi
- Hacking Smartphones
- Hacking computers
- The countermeasures you need to protect yourself from hackers
- The future of hacking
- And much, much more!

This book goes all the way from the basic principles to the intricate techniques and methods that you can use to hack. It is written to suit both beginners, as well as hacking experts. The book uses a language that beginners can understand, without leaving out the complex details that are necessary with hacking. This book is a great place to start learning how to hack and how to protect your devices. If you have been waiting for a book that can break it down for you and then dive into the deep end seamlessly, grab a copy of this book today! Buy your copy today!

A practical guide to testing your infrastructure security with Kali Linux, the preferred choice of pentesters and hackers

- Key Features
- Employ advanced pentesting techniques with Kali Linux to build highly secured systems
- Discover various stealth techniques to remain undetected and defeat modern infrastructures
- Explore red teaming techniques to exploit secured environment

Book Description This book takes you, as a tester or security practitioner, through the reconnaissance, vulnerability assessment, exploitation, privilege escalation, and post-exploitation activities used by pentesters. To start with, you'll use a

laboratory environment to validate tools and techniques, along with an application that supports a collaborative approach for pentesting. You'll then progress to passive reconnaissance with open source intelligence and active reconnaissance of the external and internal infrastructure. You'll also focus on how to select, use, customize, and interpret the results from different vulnerability scanners, followed by examining specific routes to the target, which include bypassing physical security and the exfiltration of data using a variety of techniques. You'll discover concepts such as social engineering, attacking wireless networks, web services, and embedded devices. Once you are confident with these topics, you'll learn the practical aspects of attacking user client systems by backdooring with fileless techniques, followed by focusing on the most vulnerable part of the network – directly attacking the end user. By the end of this book, you'll have explored approaches for carrying out advanced pentesting in tightly secured environments, understood pentesting and hacking techniques employed on embedded peripheral devices. What you will learn

- Configure the most effective Kali Linux tools to test infrastructure security
- Employ stealth to avoid detection in the infrastructure being tested
- Recognize when stealth attacks are being used against your infrastructure
- Exploit networks and data systems using wired and wireless networks as well as web services
- Identify and download valuable data from target systems
- Maintain access to compromised systems
- Use social engineering to compromise the weakest part of the network - the end users

Who this book is for This third edition of Mastering Kali Linux for Advanced Penetration Testing is for you if you are a security analyst, pentester, ethical hacker, IT professional, or security consultant wanting to maximize the success of your infrastructure testing using some of the advanced features of Kali Linux. Prior exposure of penetration testing and ethical hacking basics will be helpful in making the most out of this book.

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

- An overview of hacking Terminologies of hacking
- Steps to download and install Kali Linux
- The penetration testing lifecycle
- Dedicated chapters on the five stages of the penetration testing lifecycle viz. Reconnaissance, Scanning, Exploitation, Maintaining Access, and Reporting
- And a bonus chapter on Email Hacking

The book has been designed for you to understand hacking and Kali Linux from its foundation. You will not need to complete the entire book to start with a practical performance on Kali Linux. Every chapter of the penetration testing life cycle is a module in itself, and you will be in a position to try out the tools listed in them as you finish each chapter. There are step-

Online Library Advanced Penetration Testing Hacking The Worlds Most Secure Networks

by-step instructions and code snippets throughout the book that will help you get your hands dirty on a real Kali Linux system with the completion of each chapter. So here's hoping that this book helps you find the appetite to become an ethical hacker someday soon! Click the Buy Now button to get started now.

Introduces penetration testing and its importance in maintaining network security, discussing factors including the responsibilities of a penetration testing professional and potential system weaknesses.

Target, test, analyze, and report on security vulnerabilities with pen testing Pen Testing is necessary for companies looking to target, test, analyze, and patch the security vulnerabilities from hackers attempting to break into and compromise their organizations data. It takes a person with hacking skills to look for the weaknesses that make an organization susceptible to hacking. Pen Testing For Dummies aims to equip IT enthusiasts at various levels with the basic knowledge of pen testing. It is the go-to book for those who have some IT experience but desire more knowledge of how to gather intelligence on a target, learn the steps for mapping out a test, and discover best practices for analyzing, solving, and reporting on vulnerabilities. The different phases of a pen test from pre-engagement to completion Threat modeling and understanding risk When to apply vulnerability management vs penetration testing Ways to keep your pen testing skills sharp, relevant, and at the top of the game Get ready to gather intelligence, discover the steps for mapping out tests, and analyze and report results!

A practical handbook to cybersecurity for both tech and non-tech professionals As reports of major data breaches fill the headlines, it has become impossible for any business, large or small, to ignore the importance of cybersecurity. Most books on the subject, however, are either too specialized for the non-technical professional or too general for positions in the IT trenches. Thanks to author Nadean Tanner's wide array of experience from teaching at a University to working for the Department of Defense, the Cybersecurity Blue Team Toolkit strikes the perfect balance of substantive and accessible, making it equally useful to those in IT or management positions across a variety of industries. This handy guide takes a simple and strategic look at best practices and tools available to both cybersecurity management and hands-on professionals, whether they be new to the field or looking to expand their expertise. Tanner gives comprehensive coverage to such crucial topics as security assessment and configuration, strategies for protection and defense, offensive measures, and remediation while aligning the concept with the right tool using the CIS Controls version 7 as a guide. Readers will learn why and how to use fundamental open source and free tools such as ping, tracert, PuTTY, pathping, sysinternals, NMAP, OpenVAS, Nexpose Community, OSSEC, Hamachi, InSSIDer, Nexpose Community, Wireshark, Solarwinds Kiwi Syslog Server, Metasploit, Burp, Clonezilla and many more. Up-to-date and practical cybersecurity instruction, applicable to both management and technical positions • Straightforward explanations of the theory behind cybersecurity best practices • Designed to be an easily navigated tool for daily use • Includes training appendix on Linux, how to build a virtual lab and glossary of key terms The Cybersecurity Blue Team Toolkit is an excellent resource for anyone working in digital policy as well as IT security professionals, technical analysts, program managers, and Chief Information and Technology Officers. This is one handbook that won't gather dust on the shelf, but remain a valuable reference at any career level, from student to executive.

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

based programming languages such as PHP, JavaScript and MySQL will also prove helpful.

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

Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans. Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing—including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. This second version of The Hacker Playbook takes all the best "plays" from the original book and incorporates the latest attacks, tools, and lessons learned. Double the content compared to its predecessor, this guide further outlines building a lab, walks through test cases for attacks, and provides more customized code. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library—so there's no reason not to get in the game.

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.

Get to grips with security assessment, vulnerability exploitation, workload security, and encryption with this guide to ethical hacking and learn to secure your AWS environment

Key Features

- Perform cybersecurity events such as red or blue team activities and functional testing
- Gain an overview and understanding of AWS penetration testing and security
- Make the most of your AWS cloud infrastructure by learning about AWS fundamentals and exploring pentesting best practices

Book Description

Cloud security has always been treated as the highest priority by AWS while designing a robust cloud infrastructure. AWS has now extended its support to allow users and security experts to perform penetration tests on its environment. This has not only revealed a number of loopholes and brought vulnerable points in their existing system to the fore, but has also opened up opportunities for organizations to build a secure cloud environment. This book teaches you how to perform penetration tests in a controlled AWS environment. You'll begin by performing security assessments of major AWS resources such as Amazon EC2 instances, Amazon S3, Amazon API Gateway, and AWS Lambda. Throughout the course of this book, you'll also learn about specific tests such as exploiting applications, testing permissions flaws, and discovering weak policies. Moving on, you'll discover how to establish private-cloud access through backdoor Lambda functions. As you advance, you'll explore the no-go areas where users can't make changes due to vendor restrictions and find out how you can avoid being flagged to AWS in these cases. Finally, this book will take you through tips and tricks for securing your cloud environment in a professional way. By the end of this penetration testing book, you'll have become well-versed in a variety of ethical hacking techniques for securing your AWS environment against modern cyber threats. What you will learn

- Set up your AWS account and get well-versed in various pentesting services
- Delve into a variety of cloud pentesting tools and methodologies
- Discover how to exploit

vulnerabilities in both AWS and applications Understand the legality of pentesting and learn how to stay in scope Explore cloud pentesting best practices, tips, and tricks Become competent at using tools such as Kali Linux, Metasploit, and Nmap Get to grips with post-exploitation procedures and find out how to write pentesting reports Who this book is for If you are a network engineer, system administrator, or system operator looking to secure your AWS environment against external cyberattacks, then this book is for you. Ethical hackers, penetration testers, and security consultants who want to enhance their cloud security skills will also find this book useful. No prior experience in penetration testing is required; however, some understanding of cloud computing or AWS cloud is recommended.

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 dont 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.

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-defined 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.

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.

Identify tools and techniques to secure and perform a penetration test on an AWS infrastructure using Kali Linux Key Features Efficiently perform penetration testing techniques on your public cloud instances Learn not only to cover loopholes but also to automate security monitoring and alerting within your cloud-based deployment pipelines A step-by-step guide that will help you leverage the most widely used security platform to secure your AWS Cloud environment Book Description The cloud is taking over the IT industry. Any organization housing a large amount of data or a large infrastructure has started moving cloud-ward — and AWS rules the roost when it comes to cloud service providers, with its

closest competitor having less than half of its market share. This highlights the importance of security on the cloud, especially on AWS. While a lot has been said (and written) about how cloud environments can be secured, performing external security assessments in the form of pentests on AWS is still seen as a dark art. This book aims to help pentesters as well as seasoned system administrators with a hands-on approach to pentesting the various cloud services provided by Amazon through AWS using Kali Linux. To make things easier for novice pentesters, the book focuses on building a practice lab and refining penetration testing with Kali Linux on the cloud. This is helpful not only for beginners but also for pentesters who want to set up a pentesting environment in their private cloud, using Kali Linux to perform a white-box assessment of their own cloud resources. Besides this, there is a lot of in-depth coverage of the large variety of AWS services that are often overlooked during a pentest — from serverless infrastructure to automated deployment pipelines. By the end of this book, you will be able to identify possible vulnerable areas efficiently and secure your AWS cloud environment. What you will learn Familiarize yourself with and pentest the most common external-facing AWS services Audit your own infrastructure and identify flaws, weaknesses, and loopholes Demonstrate the process of lateral and vertical movement through a partially compromised AWS account Maintain stealth and persistence within a compromised AWS account Master a hands-on approach to pentesting Discover a number of automated tools to ease the process of continuously assessing and improving the security stance of an AWS infrastructure Who this book is for If you are a security analyst or a penetration tester and are interested in exploiting Cloud environments to reveal vulnerable areas and secure them, then this book is for you. A basic understanding of penetration testing, cloud computing, and its security concepts is mandatory.

Your one-stop guide to using Python, creating your own hacking tools, and making the most out of resources available for this programming language Key Features Comprehensive information on building a web application penetration testing framework using Python Master web application penetration testing using the multi-paradigm programming language Python Detect vulnerabilities in a system or application by writing your own Python scripts Book Description Python is an easy-to-learn and cross-platform programming language that has unlimited third-party libraries. Plenty of open source hacking tools are written in Python, which can be easily integrated within your script. This book is packed with step-by-step instructions and working examples to make you a skilled penetration tester. It is divided into clear bite-sized chunks, so you can learn at your own pace and focus on the areas of most interest to you. This book will teach you how to code a reverse shell and build an anonymous shell. You will also learn how to hack passwords and perform a privilege escalation on Windows with practical examples. You will set up your own virtual hacking environment in VirtualBox, which will help you run multiple operating systems for your testing environment. By the end of this book, you

will have learned how to code your own scripts and mastered ethical hacking from scratch. What you will learn Code your own reverse shell (TCP and HTTP) Create your own anonymous shell by interacting with Twitter, Google Forms, and SourceForge Replicate Metasploit features and build an advanced shell Hack passwords using multiple techniques (API hooking, keyloggers, and clipboard hijacking) Exfiltrate data from your target Add encryption (AES, RSA, and XOR) to your shell to learn how cryptography is being abused by malware Discover privilege escalation on Windows with practical examples Countermeasures against most attacks Who this book is for This book is for ethical hackers; penetration testers; students preparing for OSCP, OSCE, GPEN, GXPN, and CEH; information security professionals; cybersecurity consultants; system and network security administrators; and programmers who are keen on learning all about penetration testing.

Employ the most advanced pentesting techniques and tools to build highly-secured systems and environments About This Book Learn how to build your own pentesting lab environment to practice advanced techniques Customize your own scripts, and learn methods to exploit 32-bit and 64-bit programs Explore a vast variety of stealth techniques to bypass a number of protections when penetration testing Who This Book Is For This book is for anyone who wants to improve their skills in penetration testing. As it follows a step-by-step approach, anyone from a novice to an experienced security tester can learn effective techniques to deal with highly secured environments. Whether you are brand new or a seasoned expert, this book will provide you with the skills you need to successfully create, customize, and plan an advanced penetration test. What You Will Learn A step-by-step methodology to identify and penetrate secured environments Get to know the process to test network services across enterprise architecture when defences are in place Grasp different web application testing methods and how to identify web application protections that are deployed Understand a variety of concepts to exploit software Gain proven post-exploitation techniques to exfiltrate data from the target Get to grips with various stealth techniques to remain undetected and defeat the latest defences Be the first to find out the latest methods to bypass firewalls Follow proven approaches to record and save the data from tests for analysis In Detail The defences continue to improve and become more and more common, but this book will provide you with a number of proven techniques to defeat the latest defences on the networks. The methods and techniques contained will provide you with a powerful arsenal of best practices to increase your penetration testing successes. The processes and methodology will provide you techniques that will enable you to be successful, and the step by step instructions of information gathering and intelligence will allow you to gather the required information on the targets you are testing. The exploitation and post-exploitation sections will supply you with the tools you would need to go as far as the scope of work will allow you. The challenges at the end of each chapter are designed to challenge you and provide real-world situations that will hone and

perfect your penetration testing skills. You will start with a review of several well respected penetration testing methodologies, and following this you will learn a step-by-step methodology of professional security testing, including stealth, methods of evasion, and obfuscation to perform your tests and not be detected! The final challenge will allow you to create your own complex layered architecture with defences and protections in place, and provide the ultimate testing range for you to practice the methods shown throughout the book. The challenge is as close to an actual penetration test assignment as you can get! Style and approach The book follows the standard penetration testing stages from start to finish with step-by-step examples. The book thoroughly covers penetration test expectations, proper scoping and planning, as well as enumeration and foot printing

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

part of the network—directly and bypassing the controls, attacking the end user and maintaining persistence access through social media. You will also explore approaches to carrying out advanced penetration testing in tightly secured environments, and the book's hands-on approach will help you understand everything you need to know during a Red teaming exercise or penetration testing. Style and approach An advanced level tutorial that follows a practical approach and proven methods to maintain top notch security of your networks.

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.

This book delves deeper into analyzing the security of Docker and Kubernetes environment. This is the fourth part of the book series "Red Team: An attack paradigm".

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 as 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.

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.

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

Your pen testing career begins here, with a solid foundation in essential skills and concepts Penetration Testing Essentials provides a starting place for professionals and beginners looking to learn more about penetration testing for cybersecurity. Certification eligibility requires work experience—but before you get that experience, you need a basic understanding of the technical and behavioral ways attackers compromise security, and the tools and techniques you'll use to discover the weak spots before others do. You'll learn information gathering techniques, scanning and enumeration, how to target wireless networks, and much more as you build your pen tester skill set. You'll learn how to break in, look around, get out, and cover your tracks, all without ever being noticed. Pen testers are tremendously important to data security, so they need to be sharp and well-versed in technique, but they also need to work smarter than the average hacker. This book set you on the right path, with expert instruction from a veteran IT security expert with multiple security certifications. IT Security certifications have stringent requirements and demand a complex body of knowledge. This book lays the groundwork for any IT professional hoping to move into a cybersecurity career by developing a robust pen tester skill set. Learn the fundamentals of security and cryptography Master breaking, entering, and maintaining access to a system Escape and evade detection while covering your tracks Build your pen testing lab and the essential toolbox Start developing the tools and mindset you need to become experienced in pen testing today. A highly detailed guide to performing powerful attack vectors in many hands-on scenarios and defending significant security flaws in your company's infrastructure Key Features Advanced exploitation techniques to breach modern operating systems and complex network devices Learn about Docker breakouts, Active Directory delegation, and CRON jobs Practical use cases to deliver an intelligent endpoint-protected system Book Description It has always been difficult

to gain hands-on experience and a comprehensive understanding of advanced penetration testing techniques and vulnerability assessment and management. This book will be your one-stop solution to compromising complex network devices and modern operating systems. This book provides you with advanced penetration testing techniques that will help you exploit databases, web and application servers, switches or routers, Docker, VLAN, VoIP, and VPN. With this book, you will explore exploitation abilities such as offensive PowerShell tools and techniques, CI servers, database exploitation, Active Directory delegation, kernel exploits, cron jobs, VLAN hopping, and Docker breakouts. Moving on, this book will not only walk you through managing vulnerabilities, but will also teach you how to ensure endpoint protection. Toward the end of this book, you will also discover post-exploitation tips, tools, and methodologies to help your organization build an intelligent security system. By the end of this book, you will have mastered the skills and methodologies needed to breach infrastructures and provide complete endpoint protection for your system. What you will learn Exposure to advanced infrastructure penetration testing techniques and methodologies Gain hands-on experience of penetration testing in Linux system vulnerabilities and memory exploitation Understand what it takes to break into enterprise networks Learn to secure the configuration management environment and continuous delivery pipeline Gain an understanding of how to exploit networks and IoT devices Discover real-world, post-exploitation techniques and countermeasures Who this book is for If you are a system administrator, SOC analyst, penetration tester, or a network engineer and want to take your penetration testing skills and security knowledge to the next level, then this book is for you. Some prior experience with penetration testing tools and knowledge of Linux and Windows command-line syntax is beneficial.

[Copyright: 04d546b54fe76e4e6049942bdee8d536](#)