
A Web Services Vulnerability Testing Approach Based On

Ethical Hacker's Penetration Testing Guide

Building Virtual Pentesting Labs for Advanced Penetration Testing

Network Security Assessment

Learn Penetration Testing with Python 3.x

Web Penetration Testing with Kali Linux

Network Security Assessment

How to Break Web Software

Web Penetration Testing with Kali Linux

Hacking Web Services

Web Penetration Testing with Kali Linux

Penetration Tester's Open Source Toolkit

Mastering Cloud Penetration Testing

Hands-On AWS Penetration Testing with Kali Linux

Web Services Security Development and Architecture: Theoretical and Practical Issues

Web Application Security
Professional Pen Testing for Web Applications
Network Vulnerability Assessment
Hands-On Web Penetration Testing with Metasploit
Secure E-government Web Services
Penetration Testing and Network Defense
Penetration Testing Azure for Ethical Hackers
Mastering Kali Linux for Web Penetration Testing
The Penetration Tester's Guide to Web Applications
Web Penetration Testing with Kali Linux
Kali Linux Web Penetration Testing Cookbook
Web Security Testing Cookbook
Improving your Penetration Testing Skills
Testing Web Security
PowerShell for Penetration Testing
Advanced Penetration Testing for Highly-Secured Environments
Penetration Tester's Open Source Toolkit
Ultimate Penetration Testing with Nmap
Contemporary Complex Systems and Their Dependability
Hacking with Kali

Penetration Testing Basics
Hands-On Application Penetration Testing with Burp Suite
Developer's Guide to Web Application Security
Test and Analysis of Web Services
Practical Web Penetration Testing
The Art of Network Penetration Testing

*A Web Services
Vulnerability Testing
Approach Based On*

*Downloaded from
<ftp.wtvq.com> by guest*

HANCOCK GEMMA

Ethical Hacker's Penetration Testing Guide Packt Publishing Ltd

Learn how to break systems, networks, and software in order to determine where the bad guys might get in. Once the holes have been determined, this short book discusses how they can be fixed. Until they have been located, they are exposures to your organization. By

reading Penetration Testing Basics, you'll gain the foundations of a simple methodology used to perform penetration testing on systems and networks for which you are responsible. What You Will Learn Identify security vulnerabilities Use some of the top security tools to identify holes Read reports from testing tools Spot and negate common attacks Identify common Web-based attacks and exposures as well as recommendations for closing those holes Who This Book Is

For Anyone who has some familiarity with computers and an interest in information security and penetration testing.

Building Virtual Pentesting Labs for Advanced Penetration Testing Packt Publishing Ltd

Offering developers an inexpensive way to include testing as part of the development cycle, this cookbook features scores of recipes for testing Web applications, from relatively simple solutions to complex ones that combine several solutions.

Network Security Assessment Packt Publishing Ltd

Identify, exploit, and test web application security with ease Key Features Get up to speed with Metasploit and discover how to use it for

pentesting Understand how to exploit and protect your web environment effectively Learn how an exploit works and what causes vulnerabilities Book Description Metasploit has been a crucial security tool for many years. However, there are only a few modules that Metasploit has made available to the public for pentesting web applications. In this book, you'll explore another aspect of the framework - web applications - which is not commonly used. You'll also discover how Metasploit, when used with its inbuilt GUI, simplifies web application penetration testing. The book starts by focusing on the Metasploit setup, along with covering the life cycle of the penetration testing process. Then, you will explore Metasploit terminology and the web GUI, which is available in the

Metasploit Community Edition. Next, the book will take you through pentesting popular content management systems such as Drupal, WordPress, and Joomla, which will also include studying the latest CVEs and understanding the root cause of vulnerability in detail. Later, you'll gain insights into the vulnerability assessment and exploitation of technological platforms such as JBoss, Jenkins, and Tomcat. Finally, you'll learn how to fuzz web applications to find logical security vulnerabilities using third-party tools. By the end of this book, you'll have a solid understanding of how to exploit and validate vulnerabilities by working with various tools and techniques. What you will learn

Get up to speed with setting up and installing the Metasploit framework

Gain first-hand

experience of the Metasploit web interface

Use Metasploit for web-application reconnaissance

Understand how to pentest various content management systems

Pentest platforms such as JBoss, Tomcat, and Jenkins

Become well-versed with fuzzing web applications

Write and automate penetration testing reports

Who this book is for

This book is for web security analysts, bug bounty hunters, security professionals, or any stakeholder in the security sector who wants to delve into web application security testing.

Professionals who are not experts with command line tools or Kali Linux and prefer Metasploit's graphical user interface (GUI) will also find this book useful. No experience with Metasploit is required, but basic knowledge of Linux

and web application pentesting will be helpful.

Learn Penetration Testing with Python 3.x Elsevier

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.

Web Penetration Testing with Kali Linux
Manning Publications

Simulate real-world attacks using tactics, techniques, and procedures that adversaries use during cloud breaches
Key Features Understand the different Azure attack techniques and

methodologies used by hackers Find out how you can ensure end-to-end cybersecurity in the Azure ecosystem Discover various tools and techniques to perform successful penetration tests on your Azure infrastructure Book Description “If you're looking for this book, you need it.” — 5* Amazon Review Curious about how safe Azure really is? Put your knowledge to work with this practical guide to penetration testing. This book offers a no-faff, hands-on approach to exploring Azure penetration testing methodologies, which will get up and running in no time with the help of real-world examples, scripts, and ready-to-use source code. As you learn about the Microsoft Azure platform and understand how hackers can attack resources

hosted in the Azure cloud, you'll find out how to protect your environment by identifying vulnerabilities, along with extending your pentesting tools and capabilities. First, you'll be taken through the prerequisites for pentesting Azure and shown how to set up a pentesting lab. You'll then simulate attacks on Azure assets such as web applications and virtual machines from anonymous and authenticated perspectives. In the later chapters, you'll learn about the opportunities for privilege escalation in Azure tenants and ways in which an attacker can create persistent access to an environment. By the end of this book, you'll be able to leverage your ethical hacking skills to identify and implement different tools and techniques to perform successful

penetration tests on your own Azure infrastructure. What you will learn

- Identify how administrators misconfigure Azure services, leaving them open to exploitation
- Understand how to detect cloud infrastructure, service, and application misconfigurations
- Explore processes and techniques for exploiting common Azure security issues
- Use on-premises networks to pivot and escalate access within Azure
- Diagnose gaps and weaknesses in Azure security implementations
- Understand how attackers can escalate privileges in Azure AD

Who this book is for This book is for new and experienced infosec enthusiasts who want to learn how to simulate real-world Azure attacks using tactics, techniques, and procedures

(TTPs) that adversaries use in cloud breaches. Any technology professional working with the Azure platform (including Azure administrators, developers, and DevOps engineers) interested in learning how attackers exploit vulnerabilities in Azure hosted infrastructure, applications, and services will find this book useful.

Network Security Assessment

CreateSpace

This innovative new resource provides both professionals and aspiring professionals with clear guidance on how to identify and exploit common web application vulnerabilities. The book focuses on offensive security and how to attack web applications. It describes each of the Open Web Application Security Project (OWASP) top ten

vulnerabilities, including broken authentication, cross-site scripting and insecure deserialization, and details how to identify and exploit each weakness. Readers learn to bridge the gap between high-risk vulnerabilities and exploiting flaws to get shell access. The book demonstrates how to work in a professional services space to produce quality and thorough testing results by detailing the requirements of providing a best-of-class penetration testing service. It offers insight into the problem of not knowing how to approach a web app pen test and the challenge of integrating a mature pen testing program into an organization. Based on the author's many years of first-hand experience, this book provides examples of how to break into user accounts, how to breach

systems, and how to configure and wield penetration testing tools.

How to Break Web Software Packt Publishing Ltd

Evade antiviruses and bypass firewalls with the most widely used penetration testing frameworks Key FeaturesGain insights into the latest antivirus evasion techniquesSet up a complete pentesting environment using Metasploit and virtual machinesDiscover a variety of tools and techniques that can be used with Kali LinuxBook Description Penetration testing or ethical hacking is a legal and foolproof way to identify vulnerabilities in your system. With thorough penetration testing, you can secure your system against the majority of threats. This Learning Path starts with an in-depth explanation of what hacking and

penetration testing is. You'll gain a deep understanding of classical SQL and command injection flaws, and discover ways to exploit these flaws to secure your system. You'll also learn how to create and customize payloads to evade antivirus software and bypass an organization's defenses. Whether it's exploiting server vulnerabilities and attacking client systems, or compromising mobile phones and installing backdoors, this Learning Path will guide you through all this and more to improve your defense against online attacks. By the end of this Learning Path, you'll have the knowledge and skills you need to invade a system and identify all its vulnerabilities. This Learning Path includes content from the following Packt products: Web Penetration Testing

with Kali Linux - Third Edition by Juned Ahmed Ansari and Gilberto Najera-Gutierrez
 Metasploit Penetration Testing Cookbook - Third Edition by Abhinav Singh, Monika Agarwal, et al
 What you will learn
 Build and analyze Metasploit modules in Ruby
 Integrate Metasploit with other penetration testing tools
 Use server-side attacks to detect vulnerabilities in web servers and their applications
 Explore automated attacks such as fuzzing web applications
 Identify the difference between hacking a web application and network hacking
 Deploy Metasploit with the Penetration Testing Execution Standard (PTES)
 Use MSFvenom to generate payloads and backdoor files, and create shellcode
 Who this book is for
 This Learning Path is designed for security professionals, web

programmers, and pentesters who want to learn vulnerability exploitation and make the most of the Metasploit framework. Some understanding of penetration testing and Metasploit is required, but basic system administration skills and the ability to read code are a must.

Web Penetration Testing with Kali Linux Newnes

Master the art of exploiting advanced web penetration techniques with Kali Linux 2016.2
 About This Book
 Make the most out of advanced web pen-testing techniques using Kali Linux 2016.2
 Explore how Stored (a.k.a. Persistent) XSS attacks work and how to take advantage of them
 Learn to secure your application by performing advanced web based attacks. Bypass internet security

to traverse from the web to a private network. Who This Book Is For This book targets IT pen testers, security consultants, and ethical hackers who want to expand their knowledge and gain expertise on advanced web penetration techniques. Prior knowledge of penetration testing would be beneficial. What You Will Learn Establish a fully-featured sandbox for test rehearsal and risk-free investigation of applications Enlist open-source information to get a head-start on enumerating account credentials, mapping potential dependencies, and discovering unintended backdoors and exposed information Map, scan, and spider web applications using nmap/zenmap, nikto, arachni, webscarab, w3af, and NetCat for more

accurate characterization Proxy web transactions through tools such as Burp Suite, OWASP's ZAP tool, and Vega to uncover application weaknesses and manipulate responses Deploy SQL injection, cross-site scripting, Java vulnerabilities, and overflow attacks using Burp Suite, websploit, and SQLMap to test application robustness Evaluate and test identity, authentication, and authorization schemes and sniff out weak cryptography before the black hats do In Detail You will start by delving into some common web application architectures in use, both in private and public cloud instances. You will also learn about the most common frameworks for testing, such as OWASP OGT version 4, and how to use them to guide your efforts. In the next section,

you will be introduced to web pentesting with core tools and you will also see how to make web applications more secure through rigorous penetration tests using advanced features in open source tools. The book will then show you how to better hone your web pentesting skills in safe environments that can ensure low-risk experimentation with the powerful tools and features in Kali Linux that go beyond a typical script-kiddie approach. After establishing how to test these powerful tools safely, you will understand how to better identify vulnerabilities, position and deploy exploits, compromise authentication and authorization, and test the resilience and exposure applications possess. By the end of this book, you will be well-versed with the web service architecture to

identify and evade various protection mechanisms that are used on the Web today. You will leave this book with a greater mastery of essential test techniques needed to verify the secure design, development, and operation of your customers' web applications. Style and approach An advanced-level guide filled with real-world examples that will help you take your web application's security to the next level by using Kali Linux 2016.2.

Hacking Web Services Apress

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

Web Penetration Testing with Kali Linux BPB Publications

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

Penetration Tester's Open Source Toolkit

IGI Global

Rigorously test and improve the security of all your Web software! It's as certain as death and taxes: hackers will mercilessly attack your Web sites, applications, and services. If you're vulnerable, you'd better discover these attacks yourself, before the black hats do. Now, there's a definitive, hands-on guide to security-testing any Web-based software: *How to Break Web Software*. In this book, two renowned experts address every category of Web software exploit: attacks on clients, servers, state, user inputs, and more. You'll master powerful attack tools and techniques as you uncover dozens of crucial, widely exploited flaws in Web architecture and

coding. The authors reveal where to look for potential threats and attack vectors, how to rigorously test for each of them, and how to mitigate the problems you find. Coverage includes · Client vulnerabilities, including attacks on client-side validation · State-based attacks: hidden fields, CGI parameters, cookie poisoning, URL jumping, and session hijacking · Attacks on user-supplied inputs: cross-site scripting, SQL injection, and directory traversal · Language- and technology-based attacks: buffer overflows, canonicalization, and NULL string attacks · Server attacks: SQL Injection with stored procedures, command injection, and server fingerprinting · Cryptography, privacy, and attacks on Web services Your Web software is mission-critical-it

can't be compromised. Whether you're a developer, tester, QA specialist, or IT manager, this book will help you protect that software--systematically.

Mastering Cloud Penetration Testing BPB Publications

Web Services are an integral part of next generation Web applications. The development and use of these services is growing at an incredible rate, and so too are the security issues surrounding them. *Hacking Web Services* is a practical guide for understanding Web services security and assessment methodologies. Written for intermediate-to-advanced security professionals and developers, the book provides an in-depth look at new concepts and tools used for Web services security. Beginning with a brief introduction to

Web services technologies, the book discusses Web services assessment methodology, WSDL -- an XML format describing Web services as a set of endpoints operating on SOAP messages containing information -- and the need for secure coding. Various development issues and open source technologies used to secure and harden applications offering Web services are also covered. Throughout the book, detailed case studies, real-life demonstrations, and a variety of tips and techniques are used to teach developers how to write tools for Web services. If you are responsible for securing your company's Web services, this is a must read resource! [Hands-On AWS Penetration Testing with Kali Linux](#) "O'Reilly Media, Inc." Covers security basics and guides reader

through the process of testing a Web site. Explains how to analyze results and design specialized follow-up tests that focus on potential security gaps. Teaches the process of discovery, scanning, analyzing, verifying results of specialized tests, and fixing vulnerabilities.

Web Services Security Development and Architecture: Theoretical and Practical Issues Packt Publishing Ltd
The practical guide to simulating, detecting, and responding to network attacks Create step-by-step testing plans Learn to perform social engineering and host reconnaissance Evaluate session hijacking methods Exploit web server vulnerabilities Detect attempts to breach database security Use password crackers to obtain access information

Circumvent Intrusion Prevention Systems (IPS) and firewall protections and disrupt the service of routers and switches Scan and penetrate wireless networks Understand the inner workings of Trojan Horses, viruses, and other backdoor applications Test UNIX, Microsoft, and Novell servers for vulnerabilities Learn the root cause of buffer overflows and how to prevent them Perform and prevent Denial of Service attacks Penetration testing is a growing field but there has yet to be a definitive resource that instructs ethical hackers on how to perform a penetration test with the ethics and responsibilities of testing in mind. Penetration Testing and Network Defense offers detailed steps on how to emulate an outside attacker in order to assess the security

of a network. Unlike other books on hacking, this book is specifically geared towards penetration testing. It includes important information about liability issues and ethics as well as procedures and documentation. Using popular open-source and commercial applications, the book shows you how to perform a penetration test on an organization's network, from creating a test plan to performing social engineering and host reconnaissance to performing simulated attacks on both wired and wireless networks. Penetration Testing and Network Defense also goes a step further than other books on hacking, as it demonstrates how to detect an attack on a live network. By detailing the method of an attack and how to spot an attack on your network, this book better

prepares you to guard against hackers. You will learn how to configure, record, and thwart these attacks and how to harden a system to protect it against future internal and external attacks. Full of real-world examples and step-by-step procedures, this book is both an enjoyable read and full of practical advice that will help you assess network security and develop a plan for locking down sensitive data and company resources. "This book goes to great lengths to explain the various testing approaches that are used today and gives excellent insight into how a responsible penetration testing specialist executes his trade." -Bruce Murphy, Vice President, World Wide Security Services, Cisco Systems(R)

Web Application Security Packt

Publishing Ltd

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

Professional Pen Testing for Web Applications Packt Publishing Ltd

Build a network security threat model with this comprehensive learning guide
Key Features Develop a network security threat model for your organization Gain hands-on experience in working with network scanning and analyzing tools Learn to secure your network infrastructure Book Description The tech world has been taken over by digitization to a very large extent, and so it's

become extremely important for an organization to actively design security mechanisms for their network infrastructures. Analyzing vulnerabilities can be one of the best ways to secure your network infrastructure. Network Vulnerability Assessment starts with network security assessment concepts, workflows, and architectures. Then, you will use open source tools to perform both active and passive network scanning. As you make your way through the chapters, you will use these scanning results to analyze and design a threat model for network security. In the concluding chapters, you will dig deeper into concepts such as IP network analysis, Microsoft Services, and mail services. You will also get to grips with various security best practices, which

will help you build your network security mechanism. By the end of this book, you will be in a position to build a security framework fit for an organization. What you will learn

Develop a cost-effective end-to-end vulnerability management program

Implement a vulnerability management program from a governance perspective

Learn about various standards and frameworks for vulnerability assessments and penetration testing

Understand penetration testing with practical learning on various supporting tools and techniques

Gain insight into vulnerability scoring and reporting

Explore the importance of patching and security hardening

Develop metrics to measure the success of the vulnerability management program

Who this book is

for Network Vulnerability Assessment is for security analysts, threat analysts, and any security professionals responsible for developing a network threat model for an organization. This book is also for any individual who is or wants to be part of a vulnerability management team and implement an end-to-end robust vulnerability management program.

Network Vulnerability Assessment Packt Publishing Ltd

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.

Hands-On Web Penetration Testing with Metasploit

Packt Publishing Ltd
A practical guide to vulnerability assessment and mitigation with PowerShell Key Features Leverage PowerShell's unique capabilities at every stage of the Cyber Kill Chain, maximizing

your effectiveness Perform network enumeration techniques and exploit weaknesses with PowerShell's built-in and custom tools Learn how to conduct penetration testing on Microsoft Azure and AWS environments Purchase of the print or Kindle book includes a free PDF eBook Book Description PowerShell for Penetration Testing is a comprehensive guide designed to equip you with the essential skills you need for conducting effective penetration tests using PowerShell. You'll start by laying a solid foundation by familiarizing yourself with the core concepts of penetration testing and PowerShell scripting. In this part, you'll get up to speed with the fundamental scripting principles and their applications across various platforms. You'll then explore network

enumeration, port scanning, exploitation of web services, databases, and more using PowerShell tools. Hands-on exercises throughout the book will solidify your understanding of concepts and techniques. Extending the scope to cloud computing environments, particularly MS Azure and AWS, this book will guide you through conducting penetration tests in cloud settings, covering governance, reconnaissance, and networking intricacies. In the final part, post-exploitation techniques, including command-and-control structures and privilege escalation using PowerShell, will be explored. This section encompasses post-exploitation activities on both Microsoft Windows and Linux systems. By the end of this book, you'll have covered concise explanations, real-

world examples, and exercises that will help you seamlessly perform penetration testing techniques using PowerShell. What you will learn Get up to speed with basic and intermediate scripting techniques in PowerShell Automate penetration tasks, build custom scripts, and conquer multiple platforms Explore techniques to identify and exploit vulnerabilities in network services using PowerShell Access and manipulate web-based applications and services with PowerShell Find out how to leverage PowerShell for Active Directory and LDAP enumeration and exploitation Conduct effective pentests on cloud environments using PowerShell's cloud modules Who this book is for This book is for aspiring and intermediate pentesters as well as other cybersecurity

professionals looking to advance their knowledge. Anyone interested in PowerShell scripting for penetration testing will also find this book helpful. A basic understanding of IT systems and some programming experience will help you get the most out of this book.

Secure E-government Web Services John Wiley & Sons

Over 80 recipes on how to identify, exploit, and test web application security with Kali Linux 2 About This Book Familiarize yourself with the most common web vulnerabilities a web application faces, and understand how attackers take advantage of them Set up a penetration testing lab to conduct a preliminary assessment of attack surfaces and run exploits Learn how to prevent vulnerabilities in web

applications before an attacker can make the most of it Who This Book Is For This book is for IT professionals, web developers, security enthusiasts, and security professionals who want an accessible reference on how to find, exploit, and prevent security vulnerabilities in web applications. You should know the basics of operating a Linux environment and have some exposure to security technologies and tools. What You Will Learn Set up a penetration testing laboratory in a secure way Find out what information is useful to gather when performing penetration tests and where to look for it Use crawlers and spiders to investigate an entire website in minutes Discover security vulnerabilities in web applications in the web browser and

using command-line tools Improve your testing efficiency with the use of automated vulnerability scanners Exploit vulnerabilities that require a complex setup, run custom-made exploits, and prepare for extraordinary scenarios Set up Man in the Middle attacks and use them to identify and exploit security flaws within the communication between users and the web server Create a malicious site that will find and exploit vulnerabilities in the user's web browser Repair the most common web vulnerabilities and understand how to prevent them becoming a threat to a site's security In Detail Web applications are a huge point of attack for malicious hackers and a critical area for security professionals and penetration testers to lock down and secure. Kali Linux is a

Linux-based penetration testing platform and operating system that provides a huge array of testing tools, many of which can be used specifically to execute web penetration testing. This book will teach you, in the form step-by-step recipes, how to detect a wide array of vulnerabilities, exploit them to analyze their consequences, and ultimately buffer attackable surfaces so applications are more secure, for you and your users. Starting from the setup of a testing laboratory, this book will give you the skills you need to cover every stage of a penetration test: from gathering information about the system and the application to identifying vulnerabilities through manual testing and the use of vulnerability scanners to both basic and advanced exploitation

techniques that may lead to a full system compromise. Finally, we will put this into the context of OWASP and the top 10 web application vulnerabilities you are most likely to encounter, equipping you with the ability to combat them effectively. By the end of the book, you will have the required skills to identify, exploit, and prevent web application vulnerabilities. Style and approach Taking a recipe-based approach to web security, this book has been designed to cover each stage of a penetration test, with descriptions on how tools work and why certain programming or configuration practices can become security vulnerabilities that may put a whole system, or network, at risk. Each topic is presented as a sequence of tasks and contains a proper

explanation of why each task is performed and what it accomplishes.

Penetration Testing and Network Defense Wrox

Discover security posture, vulnerabilities, and blind spots ahead of the threat actor **KEY FEATURES** ● Includes illustrations and real-world examples of pentesting web applications, REST APIs, thick clients, mobile applications, and wireless networks. ● Covers numerous techniques such as Fuzzing (FFuF), Dynamic Scanning, Secure Code Review, and bypass testing. ● Practical application of Nmap, Metasploit, SQLmap, OWASP ZAP, Wireshark, and Kali Linux. **DESCRIPTION** The 'Ethical Hacker's Penetration Testing Guide' is a hands-on guide that will take you from

the fundamentals of pen testing to advanced security testing techniques. This book extensively uses popular pen testing tools such as Nmap, Burp Suite, Metasploit, SQLmap, OWASP ZAP, and Kali Linux. A detailed analysis of pentesting strategies for discovering OWASP top 10 vulnerabilities, such as cross-site scripting (XSS), SQL Injection, XXE, file upload vulnerabilities, etc., are explained. It provides a hands-on demonstration of pentest approaches for thick client applications, mobile applications (Android), network services, and wireless networks. Other techniques such as Fuzzing, Dynamic Scanning (DAST), and so on are also demonstrated. Security logging, harmful activity monitoring, and pentesting for sensitive data are also included in the

book. The book also covers web security automation with the help of writing effective python scripts. Through a series of live demonstrations and real-world use cases, you will learn how to break applications to expose security flaws, detect the vulnerability, and exploit it appropriately. Throughout the book, you will learn how to identify security risks, as well as a few modern cybersecurity approaches and popular pentesting tools. **WHAT YOU WILL LEARN**

- Expose the OWASP top ten vulnerabilities, fuzzing, and dynamic scanning.
- Get well versed with various pentesting tools for web, mobile, and wireless pentesting.
- Investigate hidden vulnerabilities to safeguard critical data and application components.
- Implement security logging,

application monitoring, and secure coding. ● Learn about various protocols, pentesting tools, and ethical hacking methods. WHO THIS BOOK IS FOR This book is intended for pen testers, ethical hackers, security analysts, cyber professionals, security consultants, and anybody interested in learning about penetration testing, tools, and methodologies. Knowing concepts of penetration testing is preferable but not required. TABLE OF CONTENTS 1. Overview of Web and Related Technologies and Understanding the Application 2. Web Penetration Testing- Through Code Review 3. Web

Penetration Testing-Injection Attacks 4. Fuzzing, Dynamic scanning of REST API and Web Application 5. Web Penetration Testing- Unvalidated Redirects/Forwards, SSRF 6. Pentesting for Authentication, Authorization Bypass, and Business Logic Flaws 7. Pentesting for Sensitive Data, Vulnerable Components, Security Monitoring 8. Exploiting File Upload Functionality and XXE Attack 9. Web Penetration Testing: Thick Client 10. Introduction to Network Pentesting 11. Introduction to Wireless Pentesting 12. Penetration Testing-Mobile App 13. Security Automation for Web Pentest 14. Setting up Pentest Lab