A Web Services Vulnerability Testing Approach Based On

Thank you extremely much for downloading **A Web Services Vulnerability Testing Approach Based On**.Most likely you have knowledge that, people have see numerous time for their favorite books when this A Web Services Vulnerability Testing Approach Based On, but stop up in harmful downloads.

Rather than enjoying a good ebook behind a mug of coffee in the afternoon, instead they juggled when some harmful virus inside their computer. **A Web Services Vulnerability Testing Approach Based On** is nearby in our digital library an online entry to it is set as public as a result you can download it instantly. Our digital library saves in combination countries, allowing you to get the most less latency era to download any of our books behind this one. Merely said, the A Web Services Vulnerability Testing Approach Based On is universally compatible subsequent to any devices to read.

The Art of Network Penetration Testing Springer
Simulate real-world attacks using tactics, techniques, and procedures that adversaries use during cloud breaches Key FeaturesUnderstand the different Azure attack techniques and methodologies used by hackersFind out how you can ensure end-to-end cybersecurity in the Azure ecosystemDiscover various tools and techniques to perform successful penetration tests on your Azure infrastructureBook 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 learnIdentify how administrators misconfigure Azure services, leaving them open to exploitationUnderstand how to detect cloud infrastructure, service, and application misconfigurationsExplore processes and techniques for exploiting common Azure security issuesUse on-premises networks to pivot and escalate access within AzureDiagnose gaps and weaknesses in Azure security implementationsUnderstand how attackers can escalate privileges in Azure ADWho 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.

Penetration Testing and Network Defense 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.

The Complete Reference to Professional Soa with Visual Studio 2005 (C# & VB 2005) .Net 3.0 Wrox

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 Tester's Open Source Toolkit

Springer Science & Business Media

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.

Mastering Cloud Penetration Testing Springer Science & Business Media

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

Mastering Kali Linux for Web Penetration Testing "O'Reilly Media, Inc."

The 4th FTRA International Conference on Computer Science and its Applications (CSA-12) will be held in Jeju, Korea on November 22~25, 2012. CSA-12 will be the most comprehensive conference focused on the various aspects of advances in computer science and its applications. CSA-12 will provide an opportunity for academic and industry professionals to discuss the latest issues and progress in the area of CSA. In addition, the conference will publish high quality papers which are closely related to the various theories and practical applications in CSA. Furthermore, we expect that the conference and its publications will be a trigger for further related research and technology improvements in this important subject. CSA-12 is the next event in a series of highly successful International Conference on Computer Science and its Applications,

previously held as CSA-11 (3rd Edition: Jeju, December, 2011), CSA-09 (2nd Edition: Jeju, December, 2009), and CSA-08 (1st Edition: Australia, October, 2008).

Hands-On Web Penetration Testing with Metasploit Packt Publishing Ltd

Build your defense against web attacks with Kali Linux, including command injection flaws, crypto implementation layers, and web application security holes Key Features Know how to set up your lab with Kali Linux Discover the core concepts of web penetration testing Get the tools and techniques you need with Kali Linux Book Description Web Penetration Testing with Kali Linux - Third Edition shows you how to set up a lab, helps you understand the nature and mechanics of attacking websites, and explains classical attacks in great depth. This edition is heavily updated for the latest Kali Linux changes and the most recent attacks. Kali Linux shines when it comes to client-side attacks and fuzzing in particular. From the start of the book, you'll be given a thorough grounding in the concepts of hacking and penetration testing, and you'll see the tools used in Kali Linux that relate to web application hacking. You'll gain a deep understanding of classicalSQL, command-injection flaws, and the many ways to exploit these flaws. Web penetration testing also needs a general overview of client-side attacks, which is rounded out by a long discussion of scripting and input validation flaws. There is also an important chapter on cryptographic implementation flaws, where we discuss the most recent problems with cryptographic layers in the networking stack. The importance of these attacks cannot be overstated, and defending against them is relevant to most internet users and, of course, penetration testers. At the end of the book, you'll use an automated technique called fuzzing to identify flaws in a web application. Finally, you'll gain an understanding of web application vulnerabilities and the ways they can be exploited using the tools in Kali Linux. What you will learn Learn how to set up your lab with Kali Linux Understand the core concepts of web penetration testing Get to know the tools and techniques you need to use with Kali Linux Identify the difference between hacking a web application and network hacking Expose vulnerabilities present in web servers and their applications using server-side attacks Understand the different techniques used to identify the flavor of web applications See standard attacks such as exploiting cross-site request forgery and cross-site scripting flaws Get an overview of the art of client-side attacks Explore automated attacks such as fuzzing web applications Who this book is for Since this book sets out to cover a large number of tools and security fields, it can work as an introduction to practical security skills for beginners in security. In addition, web programmers and also system administrators would benefit from this rigorous introduction to web penetration testing. Basic system administration skills are necessary, and the ability to read code is a must.

Hands-On AWS Penetration Testing with Kali Linux "O'Reilly Media, Inc."

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.

Hands-on Penetration Testing for Web Applications Packt Publishing Ltd

"This book's main objective is to present some of the key approaches, research lines, and challenges that exist in the field of security in SOA systems"--Provided by publisher.

Web Penetration Testing with Kali Linux Elsevier

A practical handbook for network adminstrators who need to develop and implement security assessment programs, exploring a variety of offensive technologies, explaining how to design and deploy networks that are immune to offensive tools and scripts, and detailing an efficient testing model. Original. (Intermediate)

Hands-On Application Penetration Testing with Burp Suite Simon and Schuster

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

Penetration Tester's Open Source Toolkit

Lulu.com

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.

How to Break Web Software Artech House

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 Penetration Testing with Kali Linux BPB Publications

The Complete Reference to Professional SOA with Visual Studio 2005 (C# & VB 2005) focuses on architecting and constructing enterprise-level systems. Taking advantage of the newly released Visual Studio 2005 development environment, the book assesses the current service-oriented platform and examines new ways to develop for scalability, availability, and security (which have become available with .NET 2.0). You'll get to look closely at application infrastructure in terms of flexibility, interoperability, and integration, as well as the decisions that have to be made to achieve optimum balance within your architecture.

Ethical Hacker ' s Penetration Testing Guide Packt Publishing Ltd

Test, fuzz, and break web applications and services using Burp Suite ' s powerful capabilities Key FeaturesMaster the skills to perform various types of security tests on your web applicationsGet hands-on experience working with components like scanner, proxy, intruder and much moreDiscover the best-way to penetrate and test web applicationsBook Description Burp suite is a set of graphic tools focused towards penetration testing of web applications. Burp suite is widely used for web penetration testing by many security professionals for performing different web-level security tasks. The book starts by setting up the environment to begin an application penetration test. You will be able to configure the client and apply target whitelisting. You will also learn to setup and configure Android and IOS devices to work with Burp Suite. The book will explain how various features of Burp Suite can be used to detect various vulnerabilities as part of an application penetration test. Once detection is completed and the vulnerability is confirmed, you will be able to exploit a detected vulnerability using Burp Suite. The book will also covers advanced concepts like writing extensions and macros for Burp suite. Finally, you will discover various steps that are taken to identify the target, discover weaknesses in the authentication mechanism, and finally break the authentication implementation to gain access to the administrative console of the application. By the end of this book, you will be able to effectively perform end-to-end penetration testing with Burp Suite. What you will learnSet up Burp Suite and its configurations for an application penetration testProxy application traffic from browsers and mobile devices to the serverDiscover and identify application security issues in various scenariosExploit discovered vulnerabilities to execute commandsExploit discovered

vulnerabilities to gain access to data in various datastoresWrite your own Burp Suite plugin and explore the Infiltrator moduleWrite macros to automate tasks in Burp SuiteWho this book is for If you are interested in learning how to test web applications and the web part of mobile applications using Burp, then this is the book for you. It is specifically designed to meet your needs if you have basic experience in using Burp and are now aiming to become a professional Burp user.

Web Penetration Testing with Kali Linux CreateSpace

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.

Professional Pen Testing for Web Applications Addison-Wesley Professional

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.

Building Virtual Pentesting Labs for Advanced Penetration Testing Pearson Education

The authors have here put together the first reference on all aspects of testing and validating service-oriented architectures. With contributions by leading academic and industrial research groups it offers detailed guidelines for the actual validation process. Readers will find a comprehensive survey of state-of-the-art approaches as well as techniques and tools to improve the quality of service-oriented applications. It also includes references and scenarios for future research and development.

Computer Science and its Applications Packt Publishing Ltd

Identify, exploit, and test web application security with ease Key FeaturesGet up to speed with Metasploit and discover how to use it for pentestingUnderstand how to exploit and protect your web environment effectivelyLearn how an exploit works and what causes vulnerabilitiesBook 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 learnGet up to speed with setting up and installing the Metasploit frameworkGain first-hand experience of the Metasploit web interfaceUse Metasploit for web-application reconnaissanceUnderstand how to pentest various content management systemsPentest platforms such as JBoss, Tomcat, and JenkinsBecome well-versed with fuzzing web applicationsWrite and automate penetration testing reportsWho 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.

Penetration Testing Azure for Ethical Hackers Packt Publishing Ltd

This book presents the proceedings of the Thirteenth International Conference on Dependability and Complex Systems (DepCoS-RELCOMEX), which took place in the Brun ó w Palace in Poland from 2nd to 6th July 2018. The conference has been organized at the Faculty of Electronics, Wroc ł aw University of Science and Technology since 2006, and it continues the tradition of two other events: RELCOMEX (1977 – 89) and Microcomputer School (1985 – 95). The selection of papers in these proceedings illustrates the broad variety of topics that are investigated in dependability analyses of today ' s complex systems. Dependability came naturally as a contemporary answer to new challenges in the reliability evaluation of these systems. Such systems cannot be considered only as structures (however complex and distributed) built on the basis of technical resources (hardware): their analysis must take into account a unique blend of interacting people (their needs and behaviours), networks (together with mobile properties, cloud-based systems) and a large number of users dispersed geographically and producing an unimaginable number of applications (working online). A growing number of research methods apply the latest advances in artificial intelligence (AI) and computational intelligence (CI). Today ' s complex systems are really complex and are applied in numerous different fields of contemporary life.