Python Web Penetration Testing Cookbook

Python Penetration Testing CookbookMetasploit Penetration Testing CookbookMetasploit Penetration Testing CookbookPython Web Penetration Testing CookbookMetasploit Penetration Testing CookbookBurp Suite CookbookPython Penetration Testing CookbookIoT Penetration Testing CookbookKali Linux Web Penetration Testing CookbookKali Linux Web Penetration Testing CookbookKali Linux Wireless Penetration Testing CookbookWeb Security Testing CookbookMetasploit Penetration Testing CookbookKali Linux - An Ethical Hacker's CookbookIot Penetration Testing CookbookMetasploit Penetration Testing Cookbook - Third EditionKali Linux Wireless Penetration Testing CookbookPython Penetration Testing EssentialsAdvanced Penetration Testing for Highly-Secured EnvironmentsKali Linux Web Penetration Testing Cookbook Rejah Rehim Abhinav Singh Monika Agarwal Cameron Buchanan Monika Agarwal Sunny Wear Maninder Singh Aaron Guzman Gilberto Nájera-Gutiérrez Gilberto Najera-Gutierrez Sean-Philip Oriyano Paco Hope Abhinav Singh Himanshu Sharma Aaron Guzman Daniel Teixeira Sean-Philip Oriyano Mohit Raj Lee Allen Gilberto Najera-Gutierrez

Python Penetration Testing Cookbook Metasploit Penetration Testing Cookbook Metasploit Penetration Testing Cookbook Python Web Penetration Testing Cookbook Metasploit Penetration Testing Cookbook Burp Suite Cookbook Python Penetration Testing Cookbook IoT Penetration Testing Cookbook Kali Linux Web Penetration Testing Cookbook Kali Linux Web Penetration Testing Cookbook Kali Linux Wireless Penetration Testing Cookbook Web Security Testing Cookbook Metasploit Penetration Testing Cookbook Kali Linux - An Ethical Hacker's Cookbook Iot Penetration Testing Cookbook Metasploit Penetration Testing Cookbook - Third Edition Kali Linux Wireless Penetration Testing Cookbook Python Penetration Testing Essentials Advanced Penetration Testing for Highly-Secured Environments Kali Linux Web Penetration Testing Cookbook *Rejah Rehim Abhinav Singh Monika Agarwal Cameron Buchanan Monika Agarwal Sunny Wear Maninder Singh Aaron Guzman Gilberto Nájera-Gutiérrez Gilberto Najera-Gutierrez Sean-Philip Oriyano Paco Hope Abhinav Singh Himanshu Sharma Aaron Guzman Daniel Teixeira Sean-Philip Oriyano Mohit Raj Lee Allen Gilberto Najera-Gutierrez*

over 50 hands on recipes to help you pen test networks using python discover vulnerabilities and find a recovery path about this book learn to detect and avoid various types of attack that put system privacy at risk enhance your knowledge of wireless application concepts and information gathering through practical recipes learn a pragmatic way to penetration test using python build efficient code and save time who this book is for if you are a developer with prior knowledge of using python for

penetration testing and if you want an overview of scripting tasks to consider while penetration testing this book will give you a lot of useful code for your toolkit what you will learn learn to configure python in different environment setups find an ip address from a web page using beautifulsoup and scrapy discover different types of packet sniffing script to sniff network packets master layer 2 and tcp ip attacks master techniques for exploit development for windows and linux incorporate various network and packet sniffing techniques using raw sockets and scrapy in detail penetration testing is the use of tools and code to attack a system in order to assess its vulnerabilities to external threats python allows pen testers to create their own tools since python is a highly valued pen testing language there are many native libraries and python bindings available specifically for pen testing tasks python penetration testing cookbook begins by teaching you how to extract information from web pages you will learn how to build an intrusion detection system using network sniffing techniques next you will find out how to scan your networks to ensure performance and quality and how to carry out wireless pen testing on your network to avoid cyber attacks after that we ll discuss the different kinds of network attack next you ll get to grips with designing your own torrent detection program we ll take you through common vulnerability scenarios and then cover buffer overflow exploitation so you can detect insecure coding finally you ll master pe code injection methods to safeguard your network style and approach this book takes a recipe based approach to solving real world problems in pen testing it is structured in stages from the initial assessment of a system through exploitation to post exploitation tests and provides scripts that can be used or modified for in depth penetration testing

over 80 recipes to master the most widely used penetration testing framework

this book follows a cookbook style with recipes explaining the steps for penetration testing with wlan voip and even cloud computing there is plenty of code and commands used to make your learning curve easy and quick this book targets both professional penetration testers as well as new users of metasploit who wish to gain expertise over the framework and learn an additional skill of penetration testing not limited to a particular os the book requires basic knowledge of scanning exploitation and the ruby language

this book gives you an arsenal of python scripts perfect to use or to customize your needs for each stage of the testing process each chapter takes you step by step through the methods of designing and modifying scripts to attack web apps you will learn how to collect both open and hidden information from websites to further your attacks identify vulnerabilities perform sql injections exploit cookies and enumerate poorly configured systems you will also discover how to crack encryption create payloads to mimic malware and create tools to output your findings into presentable formats for reporting to your employers

this book follows a cookbook style with recipes explaining the steps for penetration testing with wlan

voip and even cloud computing there is plenty of code and commands used to make your learning curve easy and quick this book targets both professional penetration testers as well as new users of metasploit who wish to gain expertise over the framework and learn an additional skill of penetration testing not limited to a particular os the book requires basic knowledge of scanning exploitation and the ruby language

get hands on experience in using burp suite to execute attacks and perform web assessments key featuresexplore the tools in burp suite to meet your web infrastructure security demandsconfigure burp to fine tune the suite of tools specific to the targetuse burp extensions to assist with different technologies commonly found in application stacksbook description burp suite is a java based platform for testing the security of your web applications and has been adopted widely by professional enterprise testers the burp suite cookbook contains recipes to tackle challenges in determining and exploring vulnerabilities in web applications you will learn how to uncover security flaws with various test cases for complex environments after you have configured burp for your environment you will use burp tools such as spider scanner intruder repeater and decoder among others to resolve specific problems faced by pentesters you will also explore working with various modes of burp and then perform operations on the web toward the end you will cover recipes that target specific test scenarios and resolve them using best practices by the end of the book you will be up and running with deploying burp for securing web applications what you will learnconfigure burp suite for your web applicationsperform authentication authorization business logic and data validation testingexplore session management and client side testingunderstand unrestricted file uploads and server side request forgeryexecute xml external entity attacks with burpperform remote code execution with burpwho this book is for if you are a security professional web pentester or software developer who wants to adopt burp suite for applications security this book is for you

over 60 hands on recipes to pen test networks using python to discover vulnerabilities and find a recovery pathabout this book learn to detect and avoid various types of attacks that put the privacy of a system at risk enhance your knowledge on the concepts of wireless applications and information gathering through practical recipes see a pragmatic way to penetration test using python to build efficient code and save timewho this book is forthis book is for developers who have prior knowledge of using python for pen testing if you want an overview of scripting tasks to consider while pen testing this book will give you a lot of useful code or your tool kit what you will learn find an ip address from a web page using beautifulsoup and urllib discover different types of sniffers to build an intrusion detection system create an efficient and high performance ping sweep and port scanner get to grips with making an ssid and bssid scanner perform network pen testing by attacking ddos dhcp and packet injecting fingerprint os and network applications and correlate common vulnerabilities master techniques to detect vulnerabilities in your environment and secure them incorporate various networks and packet sniffing techniques using raw sockets and scapyin detailpenetration testing is

the use of tools and code to attack a system in order to assess its vulnerabilities to external threats python allows pen testers to create their own tools since python is a highly valued pen testing language there are many native libraries and python bindings available specifically for pen testing tasks python penetration testing cookbook begins by teaching you how to extract information from web pages you will learn how to build an intrusion detection system using network sniffing techniques next you will find out how to scan your networks to ensure performance and quality and how to carry out wireless pen testing on your network to avoid cyber attacks after that we ll discuss the different kinds of attacks on the network next you ll get to grips with designing your own torrent detection program we ll take you through common vulnerability scenarios and then cover buffer overflow exploitation so you can detect insecure coding finally you ll discover pe code injection methods to safeguard your network

over 80 recipes to master iot security techniques about this book identify vulnerabilities in iot device architectures and firmware using software and hardware pentesting techniques understand radio communication analysis with concepts such as sniffing the air and capturing radio signals a recipe based guide that will teach you to pentest new and unique set of iot devices who this book is for this book targets iot developers iot enthusiasts pentesters and security professionals who are interested in learning about iot security prior knowledge of basic pentesting would be beneficial what you will learn set up an iot pentesting lab explore various threat modeling concepts exhibit the ability to analyze and exploit firmware vulnerabilities demonstrate the automation of application binary analysis for ios and android using mobsf set up a burp suite and use it for web app testing identify uart and jtag pinouts solder headers and hardware debugging get solutions to common wireless protocols explore the mobile security and firmware best practices master various advanced iot exploitation techniques and security automation in detail iot is an upcoming trend in the it industry today there are a lot of iot devices on the market but there is a minimal understanding of how to safeguard them if you are a security enthusiast or pentester this book will help you understand how to exploit and secure iot devices this book follows a recipe based approach giving you practical experience in securing upcoming smart devices it starts with practical recipes on how to analyze iot device architectures and identify vulnerabilities then it focuses on enhancing your pentesting skill set teaching you how to exploit a vulnerable iot device along with identifying vulnerabilities in iot device firmware next this book teaches you how to secure embedded devices and exploit smart devices with hardware techniques moving forward this book reveals advanced hardware pentesting techniques along with software defined radio based iot pentesting with zigbee and z wave finally this book also covers how to use new and unique pentesting techniques for different iot devices along with smart devices connected to the cloud by the end of this book you will have a fair understanding of how to use different pentesting techniques to exploit and secure various iot devices style and approach this recipe based book will teach you how to use advanced iot exploitation and security automation

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 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

discover the most common web vulnerabilities and prevent them from becoming a threat to your site s security key features familiarize yourself with the most common web vulnerabilities conduct a

preliminary assessment of attack surfaces and run exploits in your lab explore new tools in the kali linux ecosystem for web penetration testing book description 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 that provides a broad array of testing tools many of which can be used to execute web penetration testing kali linux penetration testing cookbook gives you the skills you need to cover every stage of a penetration test from gathering information about the system and application to identifying vulnerabilities through manual testing you will also cover the use of vulnerability scanners and look at basic and advanced exploitation techniques that may lead to a full system compromise you will start by setting up a testing laboratory exploring the latest features of tools included in kali linux and performing a wide range of tasks with owasp zap burp suite and other web proxies and security testing tools as you make your way through the book you will learn how to use automated scanners to find security flaws in web applications and understand how to bypass basic security controls in the concluding chapters you will look at what you have learned in the context of the open application security project 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 this book you will have acquired the skills you need to identify exploit and prevent web application vulnerabilities what you will learn set up a secure penetration testing laboratory use proxies crawlers and spiders to investigate an entire website identify cross site scripting and client side vulnerabilities exploit vulnerabilities that allow the insertion of code into web applications exploit vulnerabilities that require complex setups improve testing efficiency using automated vulnerability scanners learn how to circumvent security controls put in place to prevent attacks who this book is for kali linux penetration testing cookbook 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 the basics of operating a linux environment and prior exposure to security technologies and tools are necessary

over 60 powerful recipes to scan exploit and crack wireless networks for ethical purposes about this book expose wireless security threats through the eyes of an attacker recipes to help you proactively identify vulnerabilities and apply intelligent remediation acquire and apply key wireless pentesting skills used by industry experts who this book is for if you are a security professional administrator and a network professional who wants to enhance their wireless penetration testing skills and knowledge then this book is for you some prior experience with networking security and concepts is expected what you will learn deploy and configure a wireless cyber lab that resembles an enterprise production environment install kali linux 2017 3 on your laptop and configure the wireless adapter learn the fundamentals of commonly used wireless penetration testing techniques scan and enumerate wireless lans and access points use vulnerability scanning techniques to reveal flaws and weaknesses attack access points to gain access to critical networks in detail more and more organizations are moving towards wireless networks and wi fi is a popular choice the security of

wireless networks is more important than ever before due to the widespread usage of wi fi networks this book contains recipes that will enable you to maximize the success of your wireless network testing using the advanced ethical hacking features of kali linux this book will go through techniques associated with a wide range of wireless penetration tasks including wlan discovery scanning wep cracking wpa wpa2 cracking attacking access point systems operating system identification vulnerability mapping and validation of results you will learn how to utilize the arsenal of tools available in kali linux to penetrate any wireless networking environment you will also be shown how to identify remote services how to assess security risks and how various attacks are performed by finishing the recipes you will feel confident conducting wireless penetration tests and will be able to protect yourself or your organization from wireless security threats style and approach the book will provide the foundation principles techniques and in depth analysis to effectively master wireless penetration testing it will aid you in understanding and mastering many of the most powerful and useful wireless testing techniques in the industry

among the tests you perform on web applications security testing is perhaps the most important yet it s often the most neglected the recipes in the security testing cookbook demonstrate how developers and testers can check for the most common web security issues while conducting unit tests regression tests or exploratory tests unlike ad hoc security assessments these recipes are repeatable concise and systematic perfect for integrating into your regular test suite recipes cover the basics from observing messages between clients and servers to multi phase tests that script the login and execution of web application features by the end of the book you ll be able to build tests pinpointed at ajax functions as well as large multi step tests for the usual suspects cross site scripting and injection attacks this book helps you obtain install and configure useful and free security testing tools understand how your application communicates with users so you can better simulate attacks in your tests choose from many different methods that simulate common attacks such as sql injection cross site scripting and manipulating hidden form fields make your tests repeatable by using the scripts and examples in the recipes as starting points for automated tests don t live in dread of the midnight phone call telling you that your site has been hacked with security testing cookbook and the free tools used in the book s examples you can incorporate security coverage into your test suite and sleep in peace

over 100 recipes for penetration testing using metasploit and virtual machines key features special focus on the latest operating systems exploits and penetration testing techniques learn new anti virus evasion techniques and use metasploit to evade countermeasures automate post exploitation with autorunscript exploit android devices record audio and video send and read sms read call logs and much more build and analyze metasploit modules in ruby integrate metasploit with other penetration testing tools book description metasploit is the world s leading penetration testing tool and helps security and it professionals find exploit and validate vulnerabilities metasploit allows penetration testing automation password auditing web application scanning social engineering post exploitation

evidence collection and reporting metasploit s integration with insightvm or nexpose nessus openvas and other vulnerability scanners provides a validation solution that simplifies vulnerability prioritization and remediation reporting teams can collaborate in metasploit and present their findings in consolidated reports in this book you will go through great recipes that will allow you to start using metasploit effectively with an ever increasing level of complexity and covering everything from the fundamentals to more advanced features in metasploit this book is not just for beginners but also for professionals keen to master this awesome tool you will begin by building your lab environment setting up metasploit and learning how to perform intelligence gathering threat modeling vulnerability analysis exploitation and post exploitation all inside metasploit you will learn how to create and customize payloads to evade anti virus software and bypass an organization s defenses exploit server vulnerabilities attack client systems compromise mobile phones automate post exploitation install backdoors run keyloggers highjack webcams port public exploits to the framework create your own modules and much more what you will learn set up a complete penetration testing environment using metasploit and virtual machines master the world s leading penetration testing tool and use it in professional penetration testing make the most of metasploit with postgresql importing scan results using workspaces hosts loot notes services vulnerabilities and exploit results use metasploit with the penetration testing execution standard methodology use msfvenom efficiently to generate payloads and backdoor files and create shellcode leverage metasploit s advanced options upgrade sessions use proxies use meterpreter sleep control and change timeouts to be stealthy who this book is for if you are a security professional or pentester and want to get into vulnerability exploitation and make the most of the metasploit framework then this book is for you some prior understanding of penetration testing and metasploit is required

discover end to end penetration testing solutions to enhance your ethical hacking skills key featurespractical recipes to conduct effective penetration testing using the latest version of kali linuxleverage tools like metasploit wireshark nmap and more to detect vulnerabilities with easeconfidently perform networking and application attacks using task oriented recipesbook description many organizations have been affected by recent cyber events at the current rate of hacking it has become more important than ever 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 2018 4 2019 in addition to covering the core functionalities the book will get you off to a strong start by introducing you to the installation and configuration of kali linux which will help you to perform your tests you will also learn how to plan attack strategies and perform web application exploitation using tools such as burp and jexboss as you progress you will get to grips with performing network exploitation using metasploit sparta and wireshark the book will also help you delve into the technique of carrying out wireless and password attacks using tools such as patator john the ripper and airoscript ng later chapters will draw focus to the wide range of tools that help in forensics investigations and incident response mechanisms as you wrap up the concluding chapters

you will learn to create an optimum quality pentest report by the end of this book you will be equipped with the knowledge you need to conduct advanced penetration testing thanks to the book s crisp and task oriented recipes what you will learnlearn how to install set up and customize kali for pentesting on multiple platformspentest routers and embedded devicesget insights into fiddling around with software defined radiopwn and escalate through a corporate networkwrite good quality security reportsexplore digital forensics and memory analysis with kali linuxwho this book is for if you are an it security professional pentester or security analyst who wants to conduct advanced penetration testing techniques then this book is for you basic knowledge of kali linux is assumed

over 80 recipes to master iot security techniques about this book identify vulnerabilities in iot device architectures and firmware using software and hardware pentesting techniques understand radio communication analysis with concepts such as sniffing the air and capturing radio signals a recipe based guide that will teach you to pentest new and unique set of iot devices who this book is forthis book targets iot developers iot enthusiasts pentesters and security professionals who are interested in learning about iot security prior knowledge of basic pentesting would be beneficial what you will learn set up an iot pentesting lab explore various threat modeling concepts exhibit the ability to analyze and exploit firmware vulnerabilities demonstrate the automation of application binary analysis for ios and android using mobsf set up a burp suite and use it for web app testing identify uart and jtag pinouts solder headers and hardware debugging get solutions to common wireless protocols explore the mobile security and firmware best practices master various advanced iot exploitation techniques and security automationin detailiot is an upcoming trend in the it industry today there are a lot of iot devices on the market but there is a minimal understanding of how to safeguard them if you are a security enthusiast or pentester this book will help you understand how to exploit and secure iot devices this book follows a recipe based approach giving you practical experience in securing upcoming smart devices it starts with practical recipes on how to analyze iot device architectures and identify vulnerabilities then it focuses on enhancing your pentesting skill set teaching you how to exploit a vulnerable iot device along with identifying vulnerabilities in iot device firmware next this book teaches you how to secure embedded devices and exploit smart devices with hardware techniques moving forward this book reveals advanced hardware pentesting techniques along with software defined radio based iot pentesting with zigbee and z wave finally this book also covers how to use new and unique pentesting techniques for different iot devices along with smart devices connected to the cloud by the end of this book you will have a fair understanding of how to use different pentesting techniques to exploit and secure various iot devices style and approachthis recipe based book will teach you how to use advanced iot exploitation and security automation

over 100 recipes for penetration testing using metasploit and virtual machines about this book special focus on the latest operating systems exploits and penetration testing techniques learn new anti virus evasion techniques and use metasploit to evade countermeasures automate post exploitation with

autorunscript exploit android devices record audio and video send and read sms read call logs and much more build and analyze metasploit modules in ruby integrate metasploit with other penetration testing tools who this book is for if you are a security professional or pentester and want to get into vulnerability exploitation and make the most of the metasploit framework then this book is for you some prior understanding of penetration testing and metasploit is required what you will learn set up a complete penetration testing environment using metasploit and virtual machines master the world s leading penetration testing tool and use it in professional penetration testing make the most of metasploit with postgresql importing scan results using workspaces hosts loot notes services vulnerabilities and exploit results use metasploit with the penetration testing execution standard methodology use msfvenom efficiently to generate payloads and backdoor files and create shellcode leverage metasploit s advanced options upgrade sessions use proxies use meterpreter sleep control and change timeouts to be stealthy in detail metasploit is the world s leading penetration testing tool and helps security and it professionals find exploit and validate vulnerabilities metasploit allows penetration testing automation password auditing web application scanning social engineering post exploitation evidence collection and reporting metasploit s integration with insightvm or nexpose nessus openvas and other vulnerability scanners provides a validation solution that simplifies vulnerability prioritization and remediation reporting teams can collaborate in metasploit and present their findings in consolidated reports in this book you will go through great recipes that will allow you to start using metasploit effectively with an ever increasing level of complexity and covering everything from the fundamentals to more advanced features in metasploit this book is not just for beginners but also for professionals keen to master this awesome tool you will begin by building your lab environment setting up metasploit and learning ho

over 60 powerful recipes to scan exploit and crack wireless networks for ethical purposesabout this book expose wireless security threats through the eyes of an attacker recipes to help you proactively identify vulnerabilities and apply intelligent remediation acquire and apply key wireless pentesting skills used by industry expertswho this book is forif you are a security professional administrator and a network professional who wants to enhance their wireless penetration testing skills and knowledge then this book is for you some prior experience with networking security and concepts is expected what you will learn deploy and configure a wireless cyber lab that resembles an enterprise production environment install kali linux 2017 3 on your laptop and configure the wireless adapter learn the fundamentals of commonly used wireless penetration testing techniques scan and enumerate wireless lans and access points use vulnerability scanning techniques to reveal flaws and weaknesses attack access points to gain access to critical networksin detailmore and more organizations are moving towards wireless networks and wi fi is a popular choice the security of wireless networks is more important than ever before due to the widespread usage of wi fi networks this book contains recipes that will enable you to maximize the success of your wireless network testing using the advanced ethical hacking features of kali linux this book will go through techniques associated with a wide

range of wireless penetration tasks including wlan discovery scanning wep cracking wpa wpa2 cracking attacking access point systems operating system identification vulnerability mapping and validation of results you will learn how to utilize the arsenal of tools available in kali linux to penetrate any wireless networking environment you will also be shown how to identify remote services how to assess security risks and how various attacks are performed by finishing the recipes you will feel confident conducting wireless penetration tests and will be able to protect yourself or your organization from wireless security threats style and approachthe book will provide the foundation principles techniques and in depth analysis to effectively master wireless penetration testing it will aid you in understanding and mastering many of the most powerful and useful wireless testing techniques in the industry

this book gives you the skills you need to use python for penetration testing with the help of detailed code examples this book has been updated for python 3 6 3 and kali linux 2018 1 key features detect and avoid various attack types that put the privacy of a system at risk leverage python to build efficient code and eventually build a robust environment learn about securing wireless applications and information gathering on a web server book description this book gives you the skills you need to use python for penetration testing pentesting with the help of detailed code examples we start by exploring the basics of networking with python and then proceed to network hacking then you will delve into exploring python libraries to perform various types of pentesting and ethical hacking techniques next we delve into hacking the application layer where we start by gathering information from a website we then move on to concepts related to website hacking such as parameter tampering ddos xss and sql injection by reading this book you will learn different techniques and methodologies that will familiarize you with python pentesting techniques how to protect yourself and how to create automated programs to find the admin console sql injection and xss attacks what you will learn the basics of network pentesting including network scanning and sniffing wireless wired attacks and building traps for attack and torrent detection server footprinting and web application attacks including the xss and sql injection attack wireless frames and how to obtain information such as ssid bssid and the channel number from a wireless frame using a python script the importance of web server signatures email gathering and why knowing the server signature is the first step in hacking who this book is for if you are a python programmer a security researcher or an ethical hacker and are interested in penetration testing with the help of python then this book is for you even if you are new to the field of ethical hacking this book can help you find the vulnerabilities in your system so that you are ready to tackle any kind of attack or intrusion

an intensive hands on guide to perform professional penetration testing for highly secured environments from start to finish you will learn to provide penetration testing services to clients with mature security infrastructure understand how to perform each stage of the penetration test by gaining hands on experience in performing attacks that mimic those seen in the wild in the end take

the challenge and perform a virtual penetration test against a fictional corporation if you are looking for guidance and detailed instructions on how to perform a penetration test from start to finish are looking to build out your own penetration testing lab or are looking to improve on your existing penetration testing skills this book is for you although the books attempts to accommodate those that are still new to the penetration testing field experienced testers should be able to gain knowledge and hands on experience as well the book does assume that you have some experience in web application testing and as such the chapter regarding this subject may require you to understand the basic concepts of web security the reader should also be familiar with basic it concepts and commonly used protocols such as tcp ip

Introduction

The digital age has revolutionized the way we read, making books more accessible than ever. With the rise of ebooks, readers can now carry entire libraries in their pockets. Among the various sources for ebooks, free ebook sites have emerged as a popular choice. These sites offer a treasure trove of knowledge and entertainment without the cost. But what makes these sites so valuable, and where can you find the best ones? Let's dive into the world of free ebook sites.

Benefits of Free Ebook Sites

When it comes to reading, free ebook sites offer numerous advantages.

Cost Savings

First and foremost, they save you money. Buying books can be expensive, especially if you're an avid reader. Free ebook sites allow you to access a vast array of books without spending a dime.

Accessibility

These sites also enhance accessibility. Whether you're at home, on the go, or halfway around the world, you can access your favorite titles anytime, anywhere, provided you have an internet connection.

Variety of Choices

Moreover, the variety of choices available is astounding. From classic literature to contemporary novels, academic texts to children's books, free ebook sites cover all genres and interests.

Top Free Ebook Sites

There are countless free ebook sites, but a few stand out for their quality and range of offerings.

Project Gutenberg

Project Gutenberg is a pioneer in offering free ebooks. With over 60,000 titles, this site provides a wealth of classic literature in the public domain.

Open Library

Open Library aims to have a webpage for every book ever published. It offers millions of free ebooks, making it a fantastic resource for readers.

Google Books

Google Books allows users to search and preview millions of books from libraries and publishers worldwide. While not all books are available for free, many are.

ManyBooks

ManyBooks offers a large selection of free ebooks in various genres. The site is user-friendly and offers books in multiple formats.

BookBoon

BookBoon specializes in free textbooks and business books, making it an excellent resource for students and professionals.

How to Download Ebooks Safely

Downloading ebooks safely is crucial to avoid pirated content and protect your devices.

Avoiding Pirated Content

Stick to reputable sites to ensure you're not downloading pirated content. Pirated ebooks not only harm authors and publishers but can also pose security risks.

Ensuring Device Safety

Always use antivirus software and keep your devices updated to protect against malware that can be hidden in downloaded files.

Legal Considerations

Be aware of the legal considerations when downloading ebooks. Ensure the site has the right to distribute the book and that you're not violating copyright laws.

Using Free Ebook Sites for Education

Free ebook sites are invaluable for educational purposes.

Academic Resources

Sites like Project Gutenberg and Open Library offer numerous academic resources, including textbooks and scholarly articles.

Learning New Skills

You can also find books on various skills, from cooking to programming, making these sites great for personal development.

Supporting Homeschooling

For homeschooling parents, free ebook sites provide a wealth of educational materials for different grade levels and subjects.

Genres Available on Free Ebook Sites

The diversity of genres available on free ebook sites ensures there's something for everyone.

Fiction

From timeless classics to contemporary bestsellers, the fiction section is brimming with options.

Non-Fiction

Non-fiction enthusiasts can find biographies, self-help books, historical texts, and more.

Textbooks

Students can access textbooks on a wide range of subjects, helping reduce the financial burden of education.

Children's Books

Parents and teachers can find a plethora of children's books, from picture books to young adult novels.

Accessibility Features of Ebook Sites

Ebook sites often come with features that enhance accessibility.

Audiobook Options

Many sites offer audiobooks, which are great for those who prefer listening to reading.

Adjustable Font Sizes

You can adjust the font size to suit your reading comfort, making it easier for those with visual impairments.

Text-to-Speech Capabilities

Text-to-speech features can convert written text into audio, providing an alternative way to enjoy books.

Tips for Maximizing Your Ebook Experience

To make the most out of your ebook reading experience, consider these tips.

Choosing the Right Device

Whether it's a tablet, an e-reader, or a smartphone, choose a device that offers a comfortable reading experience for you.

Organizing Your Ebook Library

Use tools and apps to organize your ebook collection, making it easy to find and access your favorite titles.

Syncing Across Devices

Many ebook platforms allow you to sync your library across multiple devices, so you can pick up right where you left off, no matter which device you're using.

Challenges and Limitations

Despite the benefits, free ebook sites come with challenges and limitations.

Quality and Availability of Titles

Not all books are available for free, and sometimes the quality of the digital copy can be poor.

Digital Rights Management (DRM)

DRM can restrict how you use the ebooks you download, limiting sharing and transferring between devices.

Internet Dependency

Accessing and downloading ebooks requires an internet connection, which can be a limitation in areas with poor connectivity.

Future of Free Ebook Sites

The future looks promising for free ebook sites as technology continues to advance.

Technological Advances

Improvements in technology will likely make accessing and reading ebooks even more seamless and enjoyable.

Expanding Access

Efforts to expand internet access globally will

help more people benefit from free ebook sites.

Role in Education

As educational resources become more digitized, free ebook sites will play an increasingly vital role in learning.

Conclusion

In summary, free ebook sites offer an incredible opportunity to access a wide range of books without the financial burden. They are invaluable resources for readers of all ages and interests, providing educational materials, entertainment, and accessibility features. So why not explore these sites and discover the wealth of knowledge they offer?

FAQs

Are free ebook sites legal? Yes, most free ebook sites are legal. They typically offer books that are in the public domain or have the rights to distribute them. How do I know if an ebook site is safe? Stick to well-known and reputable sites like Project Gutenberg, Open Library, and Google Books. Check reviews and ensure the site has proper security measures. Can I download ebooks to any device? Most free ebook sites offer downloads in multiple formats, making them compatible with various devices like e-readers, tablets, and smartphones. Do free ebook sites offer audiobooks? Many free ebook sites offer audiobooks, which are perfect for those who prefer listening to their books. How can I support authors if I use free ebook sites? You can support authors by purchasing their books when possible, leaving reviews, and sharing their work with others.