
Kali Linux Ctf Blueprints

Kali Linux Network Scanning Cookbook
Die Entstaatlichung des Geldes
Handbuch Wort und Wortschatz
Grundfragen des Strafrechts, Rechtsphilosophie und die Reform der Juristenausbildung
Sag Nein ohne Skrupel
Bibel Teutsch
Die Kunst der Täuschung
Make: Elektronik
Der Turing Omnibus
Immer Elmar!
SQL-Grundlagen
Die Kunst des Human Hacking: Social Engineering-Deutsche Ausgabe
Mehr Hacking mit Python
PHP and MySQL für Dummies
Struts 2 im Einsatz
Agile Business Intelligence
Abwehrfermente
The Pentester BluePrint
Statistik von Kopf bis Fuß
Das Phantom im Netz
Das Kapital des Staates
Schnittstellenprogrammierung in SAP ABAP
Kali Linux CTF Blueprints
Learning zANTI2 for Android Pentesting
Die Kunst des Einbruchs
Kali Linux 2 - Assuring Security by Penetration Testing
Hacking
Shadowrun: Im Schatten der Drachen (ADL-Abenteureranthologie)
SAP BW/4HANA und BW auf HANA
Python Web Penetration Testing Cookbook
Die Kunst der Anonymität im Internet
Windows Internals
Cybersecurity Best Practices
Node.js High Performance
Makroökonomik in globaler Sicht
Anne und die schwarzen Katzen
Einführung in SAP BusinessObjects Web Intelligence
Deutsche Wehrmachtpsychologie 1914-1945

MAYRA AHMED

Kali Linux Network Scanning Cookbook O'Reilly Germany
Taking a highly practical approach and a playful tone, Kali Linux CTF Blueprints provides step-by-step guides to setting up vulnerabilities, in-depth guidance to exploiting them, and a variety of advice and ideas to build and customising your own challenges. If you are a penetration testing team leader or individual who wishes to challenge yourself or your friends in the creation of penetration testing assault courses, this is the book for you. The book assumes a basic level of penetration skills and familiarity with the Kali Linux operating system.

Die Entstaatlichung des Geldes dpunkt.verlag
In Anlehnung an Friedrich A. von Hayeks Werk "Die Entnationalisierung des Geldes" werden verschiedene Geldsysteme diskutiert, die den Einfluss des Staates auf das Geld entweder beschränken oder gänzlich beenden. Die Entstaatlichung durch eine konstitutionelle Bindung der Notenbank und die Verankerung einer Präferenz der Geldstabilität wird durch mehrere Beiträge verdeutlicht. Die Notwendigkeit einer weitergehenden Entstaatlichung durch mehr Wettbewerb wird auch vor dem Hintergrund der Eurokrise behandelt. Zentralbanken werden infrage gestellt, die Folgen der Institution eines reinen Zwangsgeldes werden aufgezeigt und der Währungswettbewerb wird als Lösung verteidigt. Mit Beiträgen von: Philipp Bagus, Ernst Baltensperger, James Buchanan, Milton Friedman, Friedrich A. von Hayek, Guido Hülsmann, Ekkehard Köhler, Gerald O'Driscoll, Anna Schwartz, Gerhard Schwarz, Erich Weede.

Handbuch Wort und Wortschatz Packt Publishing Ltd
Möchtest du Elektronik-Grundwissen auf eine unterhaltsame und geschmeidige Weise lernen? Mit diesem Buch tauchst du sofort in die faszinierende Welt der Elektronik ein. Entdecke die Elektronik und verstehe ihre Gesetze durch beeindruckende Experimente: Zuerst baust du etwas zusammen (oder machst etwas absichtlich kaputt) ... dann erst kommt die Theorie! Vom Einfachen zum Komplexen: Du beginnst mit einfachen Anwendungen und gehst

dann zügig über zu immer komplexeren Projekten: vom einfachen Stromkreis zum Integrierten Schaltkreis (IC), vom simplen Alarmsignal zum programmierbaren Mikrocontroller. Schritt-für-Schritt-Anleitungen und über 500 farbige Abbildungen und Fotos helfen dir dabei, Elektronik einzusetzen - und zu verstehen. Was auf dich wartet: • Entdecken durch kaputt machen: Experimentiere mit Komponenten und lerne durch Fehler • Schaff dir deine eigene, coole Arbeitsumgebung mit den Werkzeugen, die du wirklich brauchst • Erwirb Wissen über elektronische Bauelemente und ihre Bedeutung für Schaltkreise • Bau eine Alarmanlage, Lichterketten, Elektronik-Schmuck, Audioprozessoren, ein Reflextestgerät und ein Kombinations Schloss • Erhalte klare, leicht verständliche Erklärungen über das, was du tust, und warum du es so machst. Neu in der 2. Auflage: • Komplette neue Text, mit vielen neuen und überarbeiteten Projekten • Weniger und preiswertere Elektronikkomponenten • Jetzt auch mit Arduino-Experimenten
Grundfragen des Strafrechts, Rechtsphilosophie und die Reform der Juristenausbildung dpunkt.verlag
Kali Linux Network Scanning Cookbook is intended for information security professionals and casual security enthusiasts alike. It will provide the foundational principles for the novice reader but will also introduce scripting techniques and in-depth analysis for the more advanced audience. Whether you are brand new to Kali Linux or a seasoned veteran, this book will aid in both understanding and ultimately mastering many of the most powerful and useful scanning techniques in the industry. It is assumed that the reader has some basic security testing experience.

Sag Nein ohne Skrupel Packt Publishing Ltd
JUMPSTART YOUR NEW AND EXCITING CAREER AS A PENETRATION TESTER The Pentester BluePrint: Your Guide to Being a Pentester offers readers a chance to delve deeply into the world of the ethical, or "white-hat" hacker. Accomplished pentester and author Phillip L. Wylie and cybersecurity researcher Kim Crawley walk you through the basic and advanced topics necessary to understand how to make a career out of finding vulnerabilities in systems, networks, and applications. You'll learn about the role of a penetration tester, what a pentest involves,

and the prerequisite knowledge you'll need to start the educational journey of becoming a pentester. Discover how to develop a plan by assessing your current skillset and finding a starting place to begin growing your knowledge and skills. Finally, find out how to become employed as a pentester by using social media, networking strategies, and community involvement. Perfect for IT workers and entry-level information security professionals, The Pentester BluePrint also belongs on the bookshelves of anyone seeking to transition to the exciting and in-demand field of penetration testing. Written in a highly approachable and accessible style, The Pentester BluePrint avoids unnecessarily technical lingo in favor of concrete advice and practical strategies to help you get your start in pentesting. This book will teach you: The foundations of pentesting, including basic IT skills like operating systems, networking, and security systems The development of hacking skills and a hacker mindset Where to find educational options, including college and university classes, security training providers, volunteer work, and self-study Which certifications and degrees are most useful for gaining employment as a pentester How to get experience in the pentesting field, including labs, CTFs, and bug bounties
Bibel Deutsch Packt Publishing Ltd
Mitnick führt den Leser in die Denk- und Handlungsweise des Social Engineering ein, beschreibt konkrete Betrugsszenarien und zeigt eindrucksvoll die dramatischen Konsequenzen, die sich daraus ergeben. Dabei nimmt Mitnick sowohl die Perspektive des Angreifers als auch des Opfers ein und erklärt damit sehr eindrucksvoll, wieso die Täuschung so erfolgreich war - und wie man sich effektiv dagegen schützen kann.

Die Kunst der Täuschung Packt Publishing Ltd
Take your application to the next level of high performance using the extensive capabilities of Node.js About This Book Analyze, benchmark, and profile your Node.js application to find slow spots, and push it to the limit by eliminating performance bottlenecks Learn the basis of performance analysis using Node.js Explore the high performance capabilities of Node.js, along with best practices In Detail Node.js is a tool written in C, which allows you to use JavaScript on the server-side. High performance on a platform like Node.js is knowing how to take advantage of every

aspect of your hardware, helping memory management act at its best, and correctly deciding how to architect a complex application. Do not panic if your applications start consuming a lot of memory; instead spot the leak and solve it fast with Node.js by monitoring and stopping it before it becomes an issue. This book will provide you with the skills you need to analyze the performance of your application and monitor the aspects that can and should be. Starting with performance analysis concepts and their importance in helping Node.js developers eliminate performance bottlenecks, this book will take you through development patterns to avoid performance penalties. You will learn the importance of garbage collection and its behaviour, and discover how to profile your processor, allowing better performance and scalability. You will then learn about the different types of data storage methods. Moving on, you will get to grips with testing and benchmarking applications to avoid unknown application test zones. Lastly, you will explore the limits that external components can impose in your application in the form of bottlenecks. By following the examples in each chapter, you will discover tips to getting better performing applications by avoiding anti-patterns and stretching the limits of your environment as much as possible. What You Will Learn Develop applications using well-defined and well-tested development patterns Explore memory management and garbage collection to improve performance Monitor memory changes and analyze heap snapshots Profile the CPU and improve your code to avoid patterns that force intensive processor usage Understand the importance of data and when you should cache information. Learn to always test your code and benchmark when needed Extend your application's scope and know what other elements can influence performance Who This Book Is For This book is for Node.js developers who want a more in-depth knowledge of the platform to improve the performance of their applications. Whether you have a base Node.js background or you are an expert who knows the garbage collector and wants to leverage it to make applications more robust, the examples in this book will benefit you. Style and approach This is a practical guide to learning high performance, which even the least experienced developer will comprehend. Small and simple examples help you test concepts yourself and easily adapt them to any application, boosting its performance and preparing it for the real-world.

Make: Elektronik Espresso Tutorials GmbH

Achieve the gold standard in penetration testing with Kali using this masterpiece, now in its third edition! About This Book Get a rock-solid insight into penetration testing techniques and test your corporate network against threats like never before Formulate your pentesting strategies by relying on the most up-to-date and feature-rich Kali version in town—Kali Linux 2 (aka Sana). Experience this journey with new cutting-edge wireless penetration tools and a variety of new features to make your pentesting experience smoother Who This Book Is For If you are an IT security professional or a student with basic knowledge of Unix/Linux operating systems, including an awareness of information security factors, and you want to use Kali Linux for penetration testing, this book is for you. What You Will Learn Find out to download and install your own copy of Kali Linux Properly scope and conduct the initial stages of a penetration test Conduct reconnaissance and enumeration of target networks Exploit and gain a foothold on a target system or network Obtain and crack passwords Use the Kali Linux NetHunter install to conduct wireless penetration testing Create proper penetration testing reports In Detail Kali Linux is a comprehensive penetration testing platform with advanced tools to identify, detect, and exploit the vulnerabilities uncovered in the target network environment. With Kali Linux, you can apply appropriate testing methodology with defined business objectives and a scheduled test plan, resulting in a successful penetration testing project engagement. Kali Linux – Assuring Security by Penetration Testing is a fully focused, structured book providing guidance on developing practical penetration testing skills by demonstrating cutting-edge hacker tools and techniques with a coherent, step-by-step approach. This book offers you all of the essential lab preparation and testing procedures that reflect real-world attack scenarios from a business perspective, in today's digital age. Style and approach This practical guide will showcase penetration testing through cutting-edge tools and techniques using a coherent, step-by-step approach.

Der Turing Omnibus Packt Publishing Ltd

Die strukturierte Abfragesprache betrifft sowohl eine einfache als auch eine effektive Sprache, die zum Erstellen, Zugreifen auf und Bearbeiten von Daten- und Datenbankstrukturen verwendet wird. SQL (Structured Query Language) ist eine

Computerprogrammiersprache, die häufig für die Funktion mit relationalen Datenbanken verwendet wird. Der Begriff wird normalerweise als die drei Buchstaben in seiner abgekürzten Form ausgesprochen. In den 1980er Jahren entwickelte IBM SQL (Structured Query Language) als Mittel zur Kommunikation mit Datenbanken. Obwohl SQL eine strenge Syntax, Befehlsreihenfolge oder ein Wort enthält, ist es so strukturiert, dass es menschlich identifizierbar ist. Es stellt sicher, dass bestimmte grundlegende SQL-Abfragen von Nicht-Programmierern ermittelt werden. Zur besseren Lesbarkeit werden die SQL-Schlüsselwörter auch in Großbuchstaben dargestellt. Einige davon sind hier zitiert, wie FROM, WHERE und SELECT. Jedes Schlüsselwort hat eine bestimmte Inferenz, daher muss es die Datenbank in einer bestimmten Reihenfolge demonstrieren. SELECT-Anweisungen scheinen die am häufigsten verwendeten SQL-Anweisungen zu sein.

Immer Elmar! John Wiley & Sons

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.

SQL-Grundlagen MITP-Verlags GmbH & Co. KG

Wäre es nicht einfach wunderbar, wenn es ein Statistikbuch gäbe, das Histogramme, Wahrscheinlichkeitsverteilungen und Chi-Quadrat-Tests erfreulicher werden lässt als einen Zahnarztbesuch? Statistik von Kopf bis Fuß haucht diesem sonst so trockenen Fach Leben ein und vermittelt Ihnen alle Grundlagen in interaktiven, lebensnahen Szenarien, von Sportanalysen über Glücksspiele bis zum Medikamententest. Egal, ob Sie nur eine einzige Statistiklausur bestehen wollen oder sich länger und intensiver mit der Materie beschäftigen - dieses einzigartige Buchs hilft Ihnen nicht nur, sich das nötige Wissen anzueignen. Sie werden die statistischen Konzepte richtig verstehen und können Sie dann auf Fragen des täglichen Lebens anwenden. *Die Kunst des Human Hacking: Social Engineering-Deutsche*

Ausgabe Packt Publishing Ltd

Ob Sie wollen oder nicht – jede Ihrer Online-Aktivitäten wird beobachtet und analysiert Sie haben keine Privatsphäre. Im Internet ist jeder Ihrer Klicks für Unternehmen, Regierungen und kriminelle Hacker uneingeschränkt sichtbar. Ihr Computer, Ihr Smartphone, Ihr Auto, Ihre Alarmanlage, ja sogar Ihr Kühlschrank bieten potenzielle Angriffspunkte für den Zugriff auf Ihre Daten. Niemand kennt sich besser aus mit dem Missbrauch persönlicher Daten als Kevin Mitnick. Als von der US-Regierung ehemals meistgesuchter Computer-Hacker kennt er alle Schwachstellen und Sicherheitslücken des digitalen Zeitalters. Seine Fallbeispiele sind spannend und erschreckend: Sie werden Ihre Aktivitäten im Internet neu überdenken. Mitnick weiß aber auch, wie Sie Ihre Daten bestmöglich schützen. Er zeigt Ihnen anhand zahlreicher praktischer Tipps und Schritt-für-Schritt-Anleitungen, was Sie tun können, um online und offline anonym zu sein. Bestimmen Sie selbst über Ihre Daten. Lernen Sie, Ihre Privatsphäre im Internet zu schützen. Kevin Mitnick zeigt Ihnen, wie es geht. Hinterlassen Sie keine Spuren ● Sichere Passwörter festlegen und verwalten ● Mit dem Tor-Browser im Internet surfen, ohne Spuren zu hinterlassen ● E-Mails und Dateien verschlüsseln und vor fremden Zugriffen schützen ● Öffentliches WLAN, WhatsApp, Facebook & Co. sicher nutzen ● Sicherheitsrisiken vermeiden bei GPS, Smart-TV, Internet of Things und Heimautomation ● Eine zweite Identität anlegen und unsichtbar werden

Mehr Hacking mit Python BoD – Books on Demand

Der Turing Omnibus macht in 66 exzellent geschriebenen Beiträgen Station bei den interessantesten Themen aus der Informatik, der Computertechnologie und ihren Anwendungen. PHP and MySQL für Dummies Kali Linux CTF Blueprints This book provides an overview of the kill chain approach to penetration testing, and then focuses on using Kali Linux to provide examples of how this methodology is applied in the real world. After describing the underlying concepts, step-by-step examples are provided that use selected tools to demonstrate the techniques. If you are an IT professional or a security consultant who wants to maximize the success of your network testing using some of the advanced features of Kali Linux, then this book is for you. This book will teach you how to become an expert in the pre-engagement, management, and documentation of penetration testing by building on your understanding of Kali Linux and

wireless concepts.

Struts 2 im Einsatz Springer-Verlag

Die globale Ausrichtung der Makroökonomik ist der besondere Vorzug dieses Lehrwerks zweier weltberühmter Volkswirte. Für Grund- und Hauptstudium gleichermaßen zu empfehlen. Aus dem Inhalt: Grundlegende Konzepte der Makroökonomik. Bestimmung des Outputs. Konsum und Sparen. Investition. Ersparnis. Investition und Leistungsbilanz. Der staatliche Sektor. Geldnachfrage. Der Geldangebotsprozeß. Geld, Wechselkurse und Preise. Inflation. Makropolitik und Outputbestimmung in einer geschlossenen Volkswirtschaft. Makropolitik in der offenen Volkswirtschaft: feste Wechselkurse. Makropolitik in der offenen Volkswirtschaft: flexibel Wechselkurse. Inflation und Arbeitslosigkeit. Institutionelle Bestimmungsgründe von Löhnen und Arbeitslosigkeit. Zur Erklärung von Konjunkturzyklen. Langfristiges Wachstum. Theorie und Praxis der Wirtschaftspolitik. Finanzmärkte. Handelbare und nicht-handelbare Güter. Beendigung hoher Inflationen.

Agile Business Intelligence Espresso Tutorials GmbH

Das Thema Cybersecurity ist so aktuell wie nie, denn im Cyberspace lassen sich nur schwer Grenzen in Bezug auf den Zugang zu Informationen, Daten und Redefreiheit setzen. Kriminelle nutzen die Lücken oft zu ihrem Vorteil aus. Die Vielzahl der IT-Systeme, ihre unterschiedlichen Nutzungsarten und ihre Innovations- und Lebenszyklen haben zu hohen Sicherheitsrisiken für Unternehmen und staatliche Einrichtungen geführt. Diese Risiken werden sich auch langfristig nicht so einfach aus der Welt schaffen lassen. Daher müssen Institutionen Strategien und Lösungen zu ihrem Selbstschutz entwickeln. Dieses Buch beschreibt Lösungsansätze und Best Practices aus den unterschiedlichsten Bereichen, die nachweislich zu einer höheren Resilienz gegenüber Cyberangriffen führen. Weltweit renommierte IT-Sicherheitsexperten berichten in 40 Beiträgen, wie sich staatliche Institutionen, unter anderem das Militär (Cyber Defence), Behörden, internationale Organisationen und Unternehmen besser gegen Cyberangriffe schützen und nachhaltige Schutzstrategien entwickeln können. Die Autoren widmen sich den Gründen und Zielen, die ihren jeweiligen Strategien zugrunde liegen, sie berichten, wie Unternehmen auf konkrete Cyberattacken reagiert haben und wie einzelne staatliche Institutionen angesichts nationaler Cyberstrategien

agieren. In weiteren Kapiteln zeigen Wissenschaftler auf, was bei der Abwehr von Cyber-Attacken bereits heute möglich ist, welche Entwicklungen in Arbeit sind und wie diese in Zukunft eingesetzt werden können, um die Cyber-Sicherheit zu erhöhen. Im letzten Kapitel berichten Hersteller, Anwenderunternehmen und Dienstleister welche Best Practices sie in ihren Unternehmen eingeführt haben und wie andere Unternehmen ihrem Beispiel folgen können. Das Buch richtet sich an IT-Verantwortliche und -Sicherheitsbeauftragte in Unternehmen und anderen Organisationen, aber auch an Studierende in den verschiedenen IT-Studiengängen.

Abwehrfermente Walter de Gruyter GmbH & Co KG

Diese Einführung ist für ein Selbststudium in SAP BusinessObjects Web Intelligence (kurz: WeBI) ab Version 4.0 konzipiert worden, berücksichtigt jedoch auch Features, die erst in den Versionen 4.1 und 4.2 hinzu gekommen sind. Sie kann ebenso als Unterstützung für ein angeleitetes Einführungstraining herangezogen werden. Die Leser werden systematisch anhand von praktischen Beispielen und Übungsaufgaben in WeBI eingeführt. Angefangen mit elementaren Funktionalitäten erhalten sie so einen immer besseren Einblick in die Möglichkeiten zur Berichtsgestaltung. Die Kapitel beginnen jeweils mit einer praktischen Fragestellung aus dem Berichtsallday, deren Lösung durch detaillierte und gut bebilderte Klickanleitungen dargestellt wird. Anschließend erfolgt jeweils eine kurze Zusammenfassung sowie die Vermittlung vertiefenden Hintergrundwissens, um dem Benutzer auch die konzeptionelle Einordnung zu erleichtern. Am Ende des Schulungshandbuches stehen weitere Aufgaben zur Verfügung, die der Benutzer zu diesem Zeitpunkt ohne Klickanleitung lösen kann, um das bei der Bearbeitung des Buches gewonnene Verständnis zu überprüfen. Selbstverständlich sind auch die entsprechenden Lösungen zur eigenen Kontrolle vorhanden.

The Pentester BluePrint dpunkt.verlag

Nach gängiger Meinung überlässt man Innovationen am besten den dynamischen privaten Unternehmen, und der Staat hält sich raus. Das Gegenteil ist der Fall, beweist die international renommierte Ökonomin Mariana Mazzucato in ihrem in 21 Ländern veröffentlichten bahnbrechenden Buch. Der Privatsektor findet erst dann den Mut einzusteigen, wenn der unternehmerisch denkende Staat die risikoreichen Investitionen getätigt hat. »Unsere Unfähigkeit, die Rolle des Staates bei Innovation und

Wachstum anzuerkennen, könnte sehr wohl die größte Bedrohung der Entwicklung von Wohlstand sein.« Financial Times » ... auch wenn Sie mit Marianna Mazzucatos Argumenten nicht übereinstimmen, sollten Sie ihr Buch lesen: Es wird Ihr Denken verändern.« Forbes »Der Staat muss die Richtung vorgeben: Ohne aktive Industriepolitik gäbe es weder das iPhone noch das Silicon Valley, sagt die einflussreiche amerikanisch-italienische Ökonomin.« F.A.Z. »Ihre Ideen dienen Robert Habeck als Denkschule. Ein starker Staat, um Herausforderungen wie den Klimawandel zu bewältigen? Man darf gespannt sein.« Der Tagesspiegel

Statistik von Kopf bis Fuß Springer-Verlag

Der vorliegende Band enthält die auf dem Kolloquium am 25. April 2009 von Klaus Geppert, Ralf Krack und Günter Jakobs gehaltenen Vorträge und wird ergänzt durch Beiträge, die frühere und jetzige Göttinger Kollegen von Fritz Loos zu seinen Ehren verfasst haben. Die einzelnen Aufsätze versuchen mit den Generalthemen Grundfragen des Strafrechts, Rechtsphilosophie und der (unendlichen) Reform der Juristenausbildung einen Teil der Arbeitsschwerpunkte des Jubilars abzudecken. Mit dem Tagungsband verfolgen die Herausgeber das Anliegen, den Lehrer und Wissenschaftler Fritz Loos in möglichst vielen Facetten seiner Person zu würdigen und als seine akademischen Schüler Dank zu sagen für die Förderung, die er uns hat zukommen lassen.

Das Phantom im Netz MITP-Verlags GmbH & Co. KG

Related with Kali Linux Ctf Blueprints:

© [Kali Linux Ctf Blueprints United Airlines Flight Attendant Assessment](#)

© [Kali Linux Ctf Blueprints Unit Probability Homework 2 Answer Key](#)

© [Kali Linux Ctf Blueprints Unitech Training Academy West Monroe](#)

Dive into the world of advanced network penetration tests to survey and attack wireless networks using your Android device and zANTI2 About This Book Understand the basics of wireless penetration testing and its importance Learn the techniques to perform penetration testing on your wireless networks, such as scanning, detecting vulnerabilities in your victim, and then attacking This simple and intriguing guide takes a step-by-step approach that will help you get to grips with network pentesting using just your Android device and zANTI2 Who This Book Is For The book is intended for those who want to know more about network penetration tests and have no prior experience, as well as for those who are experienced in network systems and are curious to discover more about this topic. Since zANTI2 features an extremely intuitive and easy to control interface, it doesn't require any special skills. What You Will Learn Understand the importance of penetration testing throughout systems Take a run through zANTI2's interface and understand the requirements to the app Perform advanced scanning/network mapping and discover the various types of scans used on a target Discover and remotely connect to open ports on a target, thereby accessing a target's files and folders remotely Detect vulnerabilities on a target, learn how to remotely exploit them, and discover ways to protect your self from these exploits Understand what an MITM attack is and how it works, and apply this knowledge to perform attacks on network targets Learn to hijack sessions, identify

victim's passwords, replace images on websites, inject scripts, and more Use this knowledge to protect yourself from all of the attacks you will study In Detail A penetration test is one of the most important methods to secure a network or any individual machine. Having knowledge of these methods can enable a user to protect himself/herself from any kinds of attacks. Penetration tests can also be used to discover flaws or loop holes in one's security system, which if not fixed, can be exploited by an unwanted entity. This book starts off with an introduction to what penetration testing is, and how it can be performed on Android using zANTI2. Once you are aware of the basics, we move on to teach you the different types of scans that can be performed to search for targets. You will then learn how to connect to open ports and intrude into an unsecured computer. From here you will explore vulnerabilities and their usage, including ShellShock and SSL Poodle vulnerability. When connected to an open network, a user is susceptible to password and session hijacking, and a number of other cyber attacks. The book therefore ends with one of the main aspects of cyber security: the Man in the Middle attack. You will get to know everything about the MITM attack, how it works, and how one can be protected against it. Style and approach The book follows a step-by-step approach with each of the parts explained in an easy-to-follow style. Most of the methods showcased can be tried out immediately on almost any network.