

IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

If you don't fix your security vulnerabilities, attackers will exploit them. It's simply a matter of who finds them first. If you fail to prove that your software is secure, your sales are at risk too. Whether you're a technology executive, developer, or security professional, you are responsible for securing your application. However, you may be uncertain about what works, what doesn't, how hackers exploit applications, or how much to spend. Or maybe you think you do know, but don't realize what you're doing wrong. To defend against attackers, you must think like them. As a leader of ethical hackers, Ted Harrington helps the world's foremost companies secure their technology. Hackable teaches you exactly how. You'll learn how to eradicate security vulnerabilities, establish a threat model, and build security into the development process. You'll build better, more secure products. You'll gain a competitive edge, earn trust, and win sales.

Learn how to defend your ICS in practice, from lab setup and intel gathering to working with SCADA Key Features Become well-versed with offensive ways of defending your industrial control systems Learn about industrial network protocols, threat hunting, Active Directory compromises, SQL injection, and much more Build offensive and defensive skills to combat industrial cyber threats Book Description The industrial cybersecurity domain has grown significantly in recent years. To completely secure critical infrastructure, red teams must be employed to continuously test and exploit the security integrity of a company's people, processes, and products. This is a unique pentesting book, which takes a different approach by helping you gain hands-on experience with equipment that you'll come across in the field. This will enable you to understand how industrial equipment interacts and operates within an operational environment. You'll start by getting to grips with the basics of industrial processes, and then see how to create and break the process, along with gathering open-source intel to create a threat landscape for your potential customer. As you advance, you'll find out how to install and utilize offensive techniques used by professional hackers. Throughout the book, you'll explore industrial equipment, port and service discovery, pivoting, and much more, before finally launching attacks against systems in an industrial network. By the end of this penetration testing book, you'll not only understand how to analyze and navigate the intricacies of an industrial control system (ICS), but you'll also have developed essential offensive

Read PDF IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

and defensive skills to proactively protect industrial networks from modern cyberattacks. What you will learn
Set up a starter-kit ICS lab with both physical and virtual equipment
Perform open source intel-gathering pre-engagement to help map your attack landscape
Get to grips with the Standard Operating Procedures (SOPs) for penetration testing on industrial equipment
Understand the principles of traffic spanning and the importance of listening to customer networks
Gain fundamental knowledge of ICS communication
Connect physical operational technology to engineering workstations and supervisory control and data acquisition (SCADA) software
Get hands-on with directory scanning tools to map web-based SCADA solutions
Who this book is for
If you are an ethical hacker, penetration tester, automation engineer, or IT security professional looking to maintain and secure industrial networks from adversaries, this book is for you. A basic understanding of cybersecurity and recent cyber events will help you get the most out of this book.

Prepare for the CompTIA PenTest+ certification
CompTIA's PenTest+ Certification is an essential certification to building a successful penetration testing career. Test takers must pass an 85-question exam to be certified, and this book—plus the online test bank—will help you reach your certification goal.
CompTIA PenTest+ Certification For Dummies includes a map to the exam's objectives and helps you get up to speed on planning and scoping, information gathering and vulnerability identification, attacks and exploits, penetration testing tools and reporting, and communication skills. Pass the PenTest+ Certification exam and grow as a Pen Testing professional
Learn to demonstrate hands-on ability to Pen Test Practice with hundreds of study questions in a free online test bank
Find test-taking advice and a review of the types of questions you'll see on the exam
Get ready to acquire all the knowledge you need to pass the PenTest+ exam and start your career in this growing field in cybersecurity!

Take a practitioner's approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture. You'll review the architecture's central components, from hardware communication interfaces, such as UART and SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware. As the IoT rises to one of the most popular tech trends, manufacturers need to take necessary steps to secure devices and protect them from attackers. The IoT Hacker's

Read PDF IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

Handbook breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely. What You'll Learn Perform a threat model of a real-world IoT device and locate all possible attacker entry points Use reverse engineering of firmware binaries to identify security issues Analyze, assess, and identify security issues in exploited ARM and MIPS based binaries Sniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee Who This Book is For Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

Take a practitioner's approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture. You'll review the architecture's central components, from hardware communication interfaces, such as UART and SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware. As the IoT rises to one of the most popular tech trends, manufacturers need to take necessary steps to secure devices and protect them from attackers. The IoT Hacker's Handbook breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely. What You'll Learn Perform a threat model of a real-world IoT device and locate all possible attacker entry points Use reverse engineering of firmware binaries to identify security issues Analyze, assess, and identify security issues in exploited ARM and MIPS based binaries Sniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee Who This Book is For Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

Design a security framework for an Internet connected ecosystem, 2nd Edition

Mobile Application Penetration Testing

Mastering Defensive Security

Practical Web Penetration Testing

An ethical hacker's guide to analyzing, compromising, mitigating, and securing industrial processes

The Definitive Guide to Testing and Securing Deployments

Learning Pentesting for Android Devices

Kali Linux 2 is the most advanced and feature rich penetration testing

platform available. This hands-on learn by doing book will help take you beyond the basic features of Kali into a more advanced understanding of the tools and techniques used in security testing. If you have a basic understanding of Kali and want to learn more, or if you want to learn more advanced techniques, then this book is for you. Kali Linux is an Ethical Hacking platform that allows good guys to use the same tools and techniques that a hacker would use so they can find and correct security issues before the bad guys detect them. As a follow up to the popular "Basic Security Testing with Kali Linux" book, this work picks up where the first left off. Topics Include What is new in Kali 2? New Metasploit Features and Commands Creating Shells with Msfvenom Post Modules & Railgun PowerShell for Post Exploitation Web Application Pentesting How to use Burp Suite Security Testing Android Devices Forensics Tools for Security Testing Security Testing an Internet of Things (IoT) Device And much more! Explore embedded systems pentesting by applying the most common attack techniques and patterns Key Features Learn various pentesting tools and techniques to attack and secure your hardware infrastructure Find the glitches in your hardware that can be a possible entry point for attacks Discover best practices for securely designing products Book Description Hardware pentesting involves leveraging hardware interfaces and communication channels to find vulnerabilities in a device. Practical Hardware Pentesting will help you to plan attacks, hack your embedded devices, and secure the hardware infrastructure. Throughout the book, you will see how a specific device works, explore the functional and security aspects, and learn how a system senses and communicates with the outside world. You will start by setting up your lab from scratch and then gradually work with an advanced hardware lab. The book will help you get to grips with the global architecture of an embedded system and sniff on-board traffic. You will also learn how to identify and formalize threats to the embedded system and understand its relationship with its ecosystem. Later, you will discover how to analyze your hardware and locate its possible system vulnerabilities before going on to explore firmware dumping, analysis, and exploitation. Finally, focusing on the reverse engineering process from an attacker point of view will allow you to understand how devices are attacked, how they are compromised, and how you can harden a device against the most common hardware attack vectors. By the end of this book, you will be well-versed with security best practices and understand how they can be implemented to secure your hardware. What you will learn Perform an embedded system test and identify security critical functionalities Locate critical security components and buses and learn how to attack them Discover how to dump and modify stored information Understand and exploit the relationship between the firmware and hardware Identify and attack the security functions supported by the functional blocks of the device Develop an attack lab to support advanced device analysis and attacks Who this book is for This book is for security professionals and researchers who want to get started

with hardware security assessment but don't know where to start. Electrical engineers who want to understand how their devices can be attacked and how to protect against these attacks will also find this book useful.

Learn how to execute web application penetration testing end-to-end Key Features Build an end-to-end threat model landscape for web application security Learn both web application vulnerabilities and web intrusion testing Associate network vulnerabilities with a web application infrastructure Book Description Companies all over the world want to hire professionals dedicated to application security. Practical Web Penetration Testing focuses on this very trend, teaching you how to conduct application security testing using real-life scenarios. To start with, you'll set up an environment to perform web application penetration testing. You will then explore different penetration testing concepts such as threat modeling, intrusion test, infrastructure security threat, and more, in combination with advanced concepts such as Python scripting for automation. Once you are done learning the basics, you will discover end-to-end implementation of tools such as Metasploit, Burp Suite, and Kali Linux. Many companies deliver projects into production by using either Agile or Waterfall methodology. This book shows you how to assist any company with their SDLC approach and helps you on your journey to becoming an application security specialist. By the end of this book, you will have hands-on knowledge of using different tools for penetration testing. What you will learn Learn how to use Burp Suite effectively Use Nmap, Metasploit, and more tools for network infrastructure tests Practice using all web application hacking tools for intrusion tests using Kali Linux Learn how to analyze a web application using application threat modeling Know how to conduct web intrusion tests Understand how to execute network infrastructure tests Master automation of penetration testing functions for maximum efficiency using Python Who this book is for Practical Web Penetration Testing is for you if you are a security professional, penetration tester, or stakeholder who wants to execute penetration testing using the latest and most popular tools. Basic knowledge of ethical hacking would be an added advantage.

Break down the misconceptions of the Internet of Things by examining the different security building blocks available in Intel Architecture (IA) based IoT platforms. This open access book reviews the threat pyramid, secure boot, chain of trust, and the SW stack leading up to defense-in-depth. The IoT presents unique challenges in implementing security and Intel has both CPU and Isolated Security Engine capabilities to simplify it. This book explores the challenges to secure these devices to make them immune to different threats originating from within and outside the network. The requirements and robustness rules to protect the assets vary greatly and there is no single blanket solution approach to implement security. Demystifying Internet of Things Security provides clarity to industry professionals and provides an overview of different security solutions

What You'll Learn Secure devices, immunizing them against different threats originating from inside and outside the network Gather an overview of the different security building blocks available in Intel Architecture (IA) based IoT platforms Understand the threat pyramid, secure boot, chain of trust, and the software stack leading up to defense-in-depth Who This Book Is For Strategists, developers, architects, and managers in the embedded and Internet of Things (IoT) space trying to understand and implement the security in the IoT devices/platforms.

A field manual on contextualizing cyber threats, vulnerabilities, and risks to connected cars through penetration testing and risk assessment Hacking Connected Cars deconstructs the tactics, techniques, and procedures (TTPs) used to hack into connected cars and autonomous vehicles to help you identify and mitigate vulnerabilities affecting cyber-physical vehicles. Written by a veteran of risk management and penetration testing of IoT devices and connected cars, this book provides a detailed account of how to perform penetration testing, threat modeling, and risk assessments of telematics control units and infotainment systems. This book demonstrates how vulnerabilities in wireless networking, Bluetooth, and GSM can be exploited to affect confidentiality, integrity, and availability of connected cars. Passenger vehicles have experienced a massive increase in connectivity over the past five years, and the trend will only continue to grow with the expansion of The Internet of Things and increasing consumer demand for always-on connectivity. Manufacturers and OEMs need the ability to push updates without requiring service visits, but this leaves the vehicle's systems open to attack. This book examines the issues in depth, providing cutting-edge preventative tactics that security practitioners, researchers, and vendors can use to keep connected cars safe without sacrificing connectivity. Perform penetration testing of infotainment systems and telematics control units through a step-by-step methodical guide Analyze risk levels surrounding vulnerabilities and threats that impact confidentiality, integrity, and availability Conduct penetration testing using the same tactics, techniques, and procedures used by hackers From relatively small features such as automatic parallel parking, to completely autonomous self-driving cars—all connected systems are vulnerable to attack. As connectivity becomes a way of life, the need for security expertise for in-vehicle systems is becoming increasingly urgent. Hacking Connected Cars provides practical, comprehensive guidance for keeping these vehicles secure.

A Hands-On Introduction to Hacking

Internet of Things Security: Principles and Practice

Practical IoT Hacking

Advanced Infrastructure Penetration Testing

A Practical Guide to Hacking the Internet of Things

The IoT Hacker's Handbook

Bluetooth Low Energy

The huge proliferation of security vulnerability exploits, worms, and viruses

place an incredible drain on both cost and confidence for manufacturers and consumers. The release of trustworthy code requires a specific set of skills and techniques, but this information is often dispersed and decentralized, encrypted in its own jargon and terminology, Your pen testing career begins here, with a solid foundation in essential skills and concepts Penetration Testing Essentials provides a starting place for professionals and beginners looking to learn more about penetration testing for cybersecurity. Certification eligibility requires work experience—but before you get that experience, you need a basic understanding of the technical and behavioral ways attackers compromise security, and the tools and techniques you'll use to discover the weak spots before others do. You'll learn information gathering techniques, scanning and enumeration, how to target wireless networks, and much more as you build your pen tester skill set. You'll learn how to break in, look around, get out, and cover your tracks, all without ever being noticed. Pen testers are tremendously important to data security, so they need to be sharp and well-versed in technique, but they also need to work smarter than the average hacker. This book set you on the right path, with expert instruction from a veteran IT security expert with multiple security certifications. IT Security certifications have stringent requirements and demand a complex body of knowledge. This book lays the groundwork for any IT professional hoping to move into a cybersecurity career by developing a robust pen tester skill set. Learn the fundamentals of security and cryptography Master breaking, entering, and maintaining access to a system Escape and evade detection while covering your tracks Build your pen testing lab and the essential toolbox Start developing the tools and mindset you need to become experienced in pen testing today. Explore real-world threat scenarios, attacks on mobile applications, and ways to counter them About This Book Gain insights into the current threat landscape of mobile applications in particular Explore the different options that are available on mobile platforms and prevent circumventions made by attackers This is a step-by-step guide to setting up your own mobile penetration testing environment Who This Book Is For If you are a mobile application evangelist, mobile application developer, information security practitioner, penetration tester on infrastructure web applications, an application security professional, or someone who wants to learn mobile application security as a career, then this book is for you. This book will provide you with all the skills you need to get started with Android and iOS pen-testing. What You Will Learn Gain an in-depth understanding of Android and iOS architecture and the latest changes Discover how to work with different tool suites to assess any application Develop different strategies and techniques to connect to a mobile device Create a foundation for mobile application security principles Grasp techniques to attack different components of an Android device and the different functionalities of an iOS device Get to know secure

development strategies for both iOS and Android applications Gain an understanding of threat modeling mobile applications Get an in-depth understanding of both Android and iOS implementation vulnerabilities and how to provide counter-measures while developing a mobile app In Detail Mobile security has come a long way over the last few years. It has transitioned from "should it be done?" to "it must be done!" Alongside the growing number of devices and applications, there is also a growth in the volume of Personally identifiable information (PII), Financial Data, and much more. This data needs to be secured. This is why Pen-testing is so important to modern application developers. You need to know how to secure user data, and find vulnerabilities and loopholes in your application that might lead to security breaches. This book gives you the necessary skills to security test your mobile applications as a beginner, developer, or security practitioner. You'll start by discovering the internal components of an Android and an iOS application. Moving ahead, you'll understand the inter-process working of these applications. Then you'll set up a test environment for this application using various tools to identify the loopholes and vulnerabilities in the structure of the applications. Finally, after collecting all information about these security loop holes, we'll start securing our applications from these threats. Style and approach This is an easy-to-follow guide full of hands-on examples of real-world attack simulations. Each topic is explained in context with respect to testing, and for the more inquisitive, there are more details on the concepts and techniques used for different platforms.

This is an easy-to-follow guide, full of hands-on and real-world examples of applications. Each of the vulnerabilities discussed in the book is accompanied with the practical approach to the vulnerability, and the underlying security issue. This book is intended for all those who are looking to get started in Android security or Android application penetration testing. You don't need to be an Android developer to learn from this book, but it is highly recommended that developers have some experience in order to learn how to create secure applications for Android.

A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world Key Features Learn best practices to secure your data from the device to the cloud Use systems security engineering and privacy-by-design principles to design a secure IoT ecosystem A practical guide that will help you design and implement cyber security strategies for your organization Book Description With the advent of the Internet of Things (IoT), businesses have to defend against new types of threat. The business ecosystem now includes the cloud computing infrastructure, mobile and fixed endpoints that open up new attack surfaces. It therefore becomes critical to ensure that cybersecurity threats are contained to a minimum when implementing new IoT services and solutions. This book shows you how to implement cybersecurity

solutions, IoT design best practices, and risk mitigation methodologies to address device and infrastructure threats to IoT solutions. In this second edition, you will go through some typical and unique vulnerabilities seen within various layers of the IoT technology stack and also learn new ways in which IT and physical threats interact. You will then explore the different engineering approaches a developer/manufacturer might take to securely design and deploy IoT devices. Furthermore, you will securely develop your own custom additions for an enterprise IoT implementation. You will also be provided with actionable guidance through setting up a cryptographic infrastructure for your IoT implementations. You will then be guided on the selection and configuration of Identity and Access Management solutions for an IoT implementation. In conclusion, you will explore cloud security architectures and security best practices for operating and managing cross-organizational, multi-domain IoT deployments. What you will learn

Discuss the need for separate security requirements and apply security engineering principles on IoT devices

Master the operational aspects of planning, deploying, managing, monitoring, and detecting the remediation and disposal of IoT systems

Use Blockchain solutions for IoT authenticity and integrity

Explore additional privacy features emerging in the IoT industry, such as anonymity, tracking issues, and countermeasures

Design a fog computing architecture to support IoT edge analytics

Detect and respond to IoT security incidents and compromises

Who this book is for This book targets IT Security Professionals and Security Engineers (including pentesters, security architects and ethical hackers) who would like to ensure the security of their organization's data when connected through the IoT. Business analysts and managers will also find this book useful.

Demystifying Internet of Things Security

Hacking IoT

How to take over any company in the world

Advanced Penetration Testing

Secure web applications using Burp Suite, Nmap, Metasploit, and more

Penetration Testing Azure for Ethical Hackers

The Art of Network Penetration Testing

Get hands-on experience in using Burp Suite to execute attacks and perform web assessments

Key Features

Explore the tools in Burp Suite to meet your web infrastructure security demands

Configure Burp to fine-tune the suite of tools specific to the target

Use Burp extensions to assist with different technologies commonly found in application stacks

Book 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 learn

Configure Burp Suite for your web applications
Perform authentication, authorization, business logic, and data validation testing
Explore session management and client-side testing
Understand unrestricted file uploads and server-side request forgery
Execute XML external entity attacks with Burp
Perform remote code execution with Burp

Who 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 the past few years, Internet of Things has brought great changes to the world. Reports show that, the number of IoT devices is expected to reach 10 billion units within the next three years. The number will continue to rise and wildly use as infrastructure and housewares with each passing day, Therefore, ensuring the safe and stable operation of IoT devices has become more important for IoT manufacturers. Generally, four key aspects are involved in security risks when users use typical IoT products such as routers, smart speakers, and in-car entertainment systems, which are cloud, terminal, mobile device applications, and communication data. Security issues concerning any of the four may lead to the leakage of user sensitive data. Another problem is that most IoT devices are upgraded less frequently, which leads it is difficult to resolve legacy security risks in short term. In order to cope with such complex security risks, Security Companies in China, such as Qihoo 360, Xiaomi, Alibaba and Tencent, and companies in United States, e.g. Amazon, Google, Microsoft and some other companies have invested in security teams to conduct research and analyses, the findings they shared let the public become more aware of IoT device security-related risks. Currently, many IoT product suppliers have begun hiring equipment evaluation services and purchasing security protection products. As a direct participant in the IoT ecological security research project, I would like to introduce the book to anyone who is a beginner that is willing to start the IoT journey, practitioners in the IoT ecosystem, and practitioners in the security industry. This book provides beginners with key theories and methods for IoT device penetration testing; explains various tools and techniques for hardware, firmware and wireless protocol analysis; and explains how to design a secure IoT device system, while providing relevant code details.

IoT Penetration Testing Cookbook Identify vulnerabilities and secure your smart devices
Packt Publishing Ltd

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.

Internet of Things (IoT) is an ecosystem comprised of heterogeneous connected devices that communicate to deliver capabilities making our living, cities, transport, energy, and other areas more intelligent. This book delves into the different cyber-security domains and their challenges due to the massive amount and the heterogeneity of devices. This book introduces readers to the inherent concepts of IoT. It offers case studies showing how IoT counteracts the cyber-security concerns for domains. It provides suggestions on how to mitigate cyber threats by compiling a catalogue of threats that currently comprise the contemporary threat landscape. It then examines different security measures that can be applied to system installations or operational environment and discusses how these measures may alter the threat exploitability level and/or the level of the technical impact. Professionals, graduate students, researchers, academicians, and institutions that are interested in acquiring knowledge in the areas of IoT and cyber-security, will find this book of interest.

Intermediate Security Testing with Kali Linux 2

The Definitive Guide to Attacking the Internet of Things

Hacking Internet of Things

A guide to attacking embedded systems and protecting them against the most common hardware attacks

Internet of Things, Threats, Landscape, and Countermeasures

Successful IoT Device/Edge and Platform Security Deployment

Kali Linux Web Penetration Testing Cookbook

Learn the art of building a low-cost, portable hacking arsenal using Raspberry Pi 3 and Kali Linux 2 About This Book Quickly turn your Raspberry Pi 3 into a low-cost hacking tool using Kali Linux 2 Protect your confidential data by deftly preventing various network security attacks Use Raspberry Pi 3 as honeypots to warn you that hackers are on your wire Who This Book Is For If you are a computer enthusiast who wants to learn advanced hacking techniques using the Raspberry Pi 3 as your pentesting toolbox, then this book is for you. Prior knowledge of networking and Linux would be an advantage. What You Will Learn Install and tune Kali Linux 2 on a Raspberry Pi 3 for hacking Learn how to store and offload pentest data from the Raspberry Pi 3 Plan and perform man-in-the-middle attacks and bypass advanced encryption techniques Compromise systems using various exploits and tools using Kali Linux 2 Bypass security defenses and remove data off a target network Develop a command and control system to manage remotely placed Raspberry Pis Turn a Raspberry Pi 3 into a honeypot to capture sensitive information In Detail This book will show you how to utilize the latest credit card sized Raspberry Pi 3 and create a portable, low-cost hacking tool using Kali Linux 2. You'll begin by installing and tuning Kali Linux 2 on Raspberry Pi 3 and then get started with penetration testing. You will be exposed to various network security scenarios such as wireless security, scanning network packets in order to detect any issues in the network, and capturing sensitive data. You will also learn how to plan and perform various attacks such as man-in-the-middle, password cracking, bypassing SSL encryption, compromising systems using various toolkits, and many more. Finally, you'll see how to bypass security defenses and avoid detection, turn your Pi 3 into a honeypot, and develop a command and control system to manage a remotely-placed Raspberry Pi 3. By the end of this book you will be able to turn Raspberry Pi 3 into a hacking arsenal to leverage the most popular open source toolkit, Kali Linux 2.0. Style and approach This concise and fast-paced guide will ensure you get hands-on with penetration testing right from the start. You will quickly install the powerful Kali Linux 2 on your Raspberry Pi 3 and then learn how to use and conduct fundamental penetration techniques and attacks.

Skillfully navigate through the complex realm of implementing

Read PDF IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

scalable, trustworthy industrial systems and architectures in a hyper-connected business world. Key Features Gain practical insight into security concepts in the Industrial Internet of Things (IIoT) architecture Demystify complex topics such as cryptography and blockchain Comprehensive references to industry standards and security frameworks when developing IIoT blueprints Book Description Securing connected industries and autonomous systems is a top concern for the Industrial Internet of Things (IIoT) community. Unlike cybersecurity, cyber-physical security is an intricate discipline that directly ties to system reliability as well as human and environmental safety. Practical Industrial Internet of Things Security enables you to develop a comprehensive understanding of the entire spectrum of securing connected industries, from the edge to the cloud. This book establishes the foundational concepts and tenets of IIoT security by presenting real-world case studies, threat models, and reference architectures. You'll work with practical tools to design risk-based security controls for industrial use cases and gain practical know-how on the multi-layered defense techniques including Identity and Access Management (IAM), endpoint security, and communication infrastructure. Stakeholders, including developers, architects, and business leaders, can gain practical insights in securing IIoT lifecycle processes, standardization, governance and assess the applicability of emerging technologies, such as blockchain, Artificial Intelligence, and Machine Learning, to design and implement resilient connected systems and harness significant industrial opportunities. What you will learn Understand the crucial concepts of a multi-layered IIoT security framework Gain insight on securing identity, access, and configuration management for large-scale IIoT deployments Secure your machine-to-machine (M2M) and machine-to-cloud (M2C) connectivity Build a concrete security program for your IIoT deployment Explore techniques from case studies on industrial IoT threat modeling and mitigation approaches Learn risk management and mitigation planning Who this book is for Practical Industrial Internet of Things Security is for the IIoT community, which includes IIoT researchers, security professionals, architects, developers, and business stakeholders. Anyone who needs to have a comprehensive understanding of the unique safety and security challenges of connected industries and practical methodologies to secure industrial assets will find this book immensely helpful. This book is uniquely designed to benefit professionals from both IT and industrial operations backgrounds.

This book is an introduction for the reader into the wonderful world of IoT device exploitation. The book is supposed to be a

Read PDF IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

tutorial guide that helps a reader understand various skills that are required for hacking an IoT device. As the IoT trend rises to one of the most popular technical trend, manufactures need to take necessary steps to ensure that the devices are secure and protect them from attackers. This hacking guide breaks down the Internet of Things, exploits it, and reveals how these devices can be exploited. The readers will learn to tear apart various Smart devices and understand how to grab the firmware using various techniques such as UART communication, SPI/I2C transfer and also understand how to use the "chip-off" technique to read from BGA/VBGA EEPROM chip. We will learn to identify security issues such as stack and heap overflows, command injection and other web security issues within a device's network daemons. The readers will also be shown how to analyze cloud services utilized by these devices and identify security issues within them that can allow to control the device remotely. Also we will learn to analyze the accompanying mobile apps that allow them to be controlled from anywhere in the world. The readers will be learn how to do all these things above by looking at case studies of VPN Gateway device Smart router Smart home controller Smart Security cameras Smart industrial tool Smart Fitness bands At the end of the chapter we will also learn how to write simple scripts that can help automate to some extent idetifying these kind of security issues within the binaries utilized by these devices. By the end of the book we would have identified 0 or 1-day exploits within all of these devices. What You'll Learn Analyze a real-world IoT device and locate all possible attacker entry points Use reverse engineering techniques to identify security issues within firmware binaries Find 0 or 1-day exploits in various Sniff, capture, and exploit communication protocols, HTTP, custom protocols as well as Bluetooth Low Energy (BLE) Who This Book is For Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

Security and Privacy Issues in IoT Devices and Sensor Networks investigates security breach issues in IoT and sensor networks, exploring various solutions. The book follows a two-fold approach, first focusing on the fundamentals and theory surrounding sensor networks and IoT security. It then explores practical solutions that can be implemented to develop security for these elements, providing case studies to enhance understanding. Machine learning techniques are covered, as well as other security paradigms, such as cloud security and cryptocurrency technologies. The book highlights how these

Read PDF IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

techniques can be applied to identify attacks and vulnerabilities, preserve privacy, and enhance data security. This in-depth reference is ideal for industry professionals dealing with WSN and IoT systems who want to enhance the security of these systems. Additionally, researchers, material developers and technology specialists dealing with the multifarious aspects of data privacy and security enhancement will benefit from the book's comprehensive information. Provides insights into the latest research trends and theory in the field of sensor networks and IoT security Presents machine learning-based solutions for data security enhancement Discusses the challenges to implement various security techniques Informs on how analytics can be used in security and privacy

Securing the Internet of Things provides network and cybersecurity researchers and practitioners with both the theoretical and practical knowledge they need to know regarding security in the Internet of Things (IoT). This booming field, moving from strictly research to the marketplace, is advancing rapidly, yet security issues abound. This book explains the fundamental concepts of IoT security, describing practical solutions that account for resource limitations at IoT end-node, hybrid network architecture, communication protocols, and application characteristics. Highlighting the most important potential IoT security risks and threats, the book covers both the general theory and practical implications for people working in security in the Internet of Things. Helps researchers and practitioners understand the security architecture in IoT and the state-of-the-art in IoT security countermeasures Explores how the threats in IoT are different from traditional ad hoc or infrastructural networks Provides a comprehensive discussion on the security challenges and solutions in RFID, WSNs, and IoT

Contributed material by Dr. Imed Romdhani

Hacking Connected Cars

Security and Privacy Issues in IoT Devices and Sensor Networks

Practical Hardware Pentesting

Strengthen your defense against web attacks with Kali Linux and Metasploit

Pentesting Industrial Control Systems

Testing Code Security

IoT Penetration Testing Cookbook

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

Read PDF IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

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.

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

Read PDF IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

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.

Your ultimate guide to pentesting with Kali Linux Kali is a popular and powerful Linux distribution used by cybersecurity professionals around the world. Penetration testers must master Kali ' s varied library of tools to be effective at their work. The Kali Linux Penetration Testing Bible is the hands-on and methodology guide for pentesting with Kali. You ' ll discover everything you need to know about the tools and techniques hackers use to gain access to systems like yours so you can erect reliable defenses for your virtual assets. Whether you ' re new to the field or an established pentester, you ' ll find what you need in this comprehensive guide. Build a modern dockerized environment Discover the fundamentals of the bash language in Linux Use a variety of effective techniques to find vulnerabilities (OSINT, Network Scan, and more) Analyze your findings and identify false positives and uncover advanced subjects, like buffer overflow, lateral movement, and privilege escalation Apply

practical and efficient pentesting workflows Learn about Modern Web Application Security Secure SDLC Automate your penetration testing with Python

An immersive learning experience enhanced with technical, hands-on labs to understand the concepts, methods, tools, platforms, and systems required to master the art of cybersecurity Key FeaturesGet hold of the best defensive security strategies and toolsDevelop a defensive security strategy at an enterprise levelGet hands-on with advanced cybersecurity threat detection, including XSS, SQL injections, brute forcing web applications, and moreBook Description Every organization has its own data and digital assets that need to be protected against an ever-growing threat landscape that compromises the availability, integrity, and confidentiality of crucial data. Therefore, it is important to train professionals in the latest defensive security skills and tools to secure them. Mastering Defensive Security provides you with in-depth knowledge of the latest cybersecurity threats along with the best tools and techniques needed to keep your infrastructure secure. The book begins by establishing a strong foundation of cybersecurity concepts and advances to explore the latest security technologies such as Wireshark, Damn Vulnerable Web App (DVWA), Burp Suite, OpenVAS, and Nmap, hardware threats such as a weaponized Raspberry Pi, and hardening techniques for Unix, Windows, web applications, and cloud infrastructures. As you make progress through the chapters, you'll get to grips with several advanced techniques such as malware analysis, security automation, computer forensics, and vulnerability assessment, which will help you to leverage pentesting for security. By the end of this book, you'll have become familiar with creating your own defensive security tools using IoT devices and developed advanced defensive security skills. What you will learnBecome well versed with concepts related to defensive securityDiscover strategies and tools to secure the most vulnerable factor – the userGet hands-on experience using and configuring the best security toolsUnderstand how to apply hardening techniques in Windows and Unix environmentsLeverage malware analysis and forensics to enhance your security strategySecure Internet of Things (IoT) implementationsEnhance the security of web applications and cloud deploymentsWho this book is for This book is for all IT professionals who want to take their first steps into the world of defensive security; from system admins and programmers to data analysts and data scientists with an interest in security. Experienced cybersecurity professionals working on broadening their knowledge and keeping up to date with the latest defensive developments will also find plenty of useful information in this book. You'll need a basic understanding of networking, IT, servers, virtualization, and cloud platforms before you get started with this book.

Convert Android to a powerful pentesting platform. Key FeaturesGet up and running with Kali Linux NetHunter Connect your Android device and gain full control over Windows, OSX, or Linux devices Crack Wi-Fi passwords and gain

access to devices connected over the same network collecting intellectual data

Book Description Kali NetHunter is a version of the popular and powerful Kali Linux pentesting platform, designed to be installed on mobile devices. Hands-On Penetration Testing with Kali NetHunter will teach you the components of NetHunter and how to install the software. You ' ll also learn about the different tools included and how to optimize and use a package, obtain desired results, perform tests, and make your environment more secure. Starting with an introduction to Kali NetHunter, you will delve into different phases of the pentesting process. This book will show you how to build your penetration testing environment and set up your lab. You will gain insight into gathering intellectual data, exploiting vulnerable areas, and gaining control over target systems. As you progress through the book, you will explore the NetHunter tools available for exploiting wired and wireless devices. You will work through new ways to deploy existing tools designed to reduce the chances of detection. In the concluding chapters, you will discover tips and best practices for integrating security hardening into your Android ecosystem. By the end of this book, you will have learned to successfully use a mobile penetration testing device based on Kali NetHunter and Android to accomplish the same tasks you would traditionally, but in a smaller and more mobile form factor. What you will learn

- Choose and configure a hardware device to use Kali NetHunter
- Use various tools during pentests
- Understand NetHunter suite components
- Discover tips to effectively use a compact mobile platform
- Create your own Kali NetHunter-enabled device and configure it for optimal results
- Learn to scan and gather information from a target
- Explore hardware adapters for testing and auditing wireless networks and Bluetooth devices

Who this book is for Hands-On Penetration Testing with Kali NetHunter is for pentesters, ethical hackers, and security professionals who want to learn to use Kali NetHunter for complete mobile penetration testing and are interested in venturing into the mobile domain. Some prior understanding of networking assessment and Kali Linux will be helpful.

Tactics, Techniques, and Procedures

Burp Suite Cookbook

IoT Penetration Testing Cookbook

Penetration Testing For Dummies

Practical recipes to help you master web penetration testing with Burp Suite

Identify vulnerabilities and secure your smart devices

Hands-On Penetration Testing with Kali NetHunter

Simulate real-world attacks using tactics, techniques, and procedures that

adversaries use during cloud breaches

Key Features Understand the different

Azure attack techniques and methodologies used by hackers

Find out how you

can ensure end-to-end cybersecurity in the Azure ecosystem

Discover various

tools and techniques to perform successful penetration tests on your Azure

infrastructure

Book Description "If you're looking for this book, you need it." —

5* Amazon Review Curious about how safe Azure really is? Put your knowledge to work with this practical guide to penetration testing. This book offers a no-faff, hands-on approach to exploring Azure penetration testing methodologies, which will get up and running in no time with the help of real-world examples, scripts, and ready-to-use source code. As you learn about the Microsoft Azure platform and understand how hackers can attack resources hosted in the Azure cloud, you'll find out how to protect your environment by identifying vulnerabilities, along with extending your pentesting tools and capabilities. First, you'll be taken through the prerequisites for pentesting Azure and shown how to set up a pentesting lab. You'll then simulate attacks on Azure assets such as web applications and virtual machines from anonymous and authenticated perspectives. In the later chapters, you'll learn about the opportunities for privilege escalation in Azure tenants and ways in which an attacker can create persistent access to an environment. By the end of this book, you'll be able to leverage your ethical hacking skills to identify and implement different tools and techniques to perform successful penetration tests on your own Azure infrastructure. What you will learn

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

Who this book is for This book is for new and experienced infosec enthusiasts who want to learn how to simulate real-world Azure attacks using tactics, techniques, and procedures (TTPs) that adversaries use in cloud breaches. Any technology professional working with the Azure platform (including Azure administrators, developers, and DevOps engineers) interested in learning how attackers exploit vulnerabilities in Azure hosted infrastructure, applications, and services will find this book useful.

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

Read PDF IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

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. This 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

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In *Penetration Testing*, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine-based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: -Crack passwords and wireless network keys with brute-forcing and wordlists -Test web applications for vulnerabilities -Use the Metasploit Framework to launch exploits and write your own Metasploit modules -Automate social-engineering attacks -Bypass antivirus software -Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the

Read PDF IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.

LPWAN Technologies for IoT and M2M Applications provides insight into LPWAN technologies, also presenting a wide range of applications and a discussion on security issues and future challenges and research directions. This book is a beneficial and insightful resource for university researchers, graduate students and R&D engineers who are designing networks and implementing IoT applications. To support new requirements for this emerging industry, a new paradigm of Low Power Wide Area Networks (LPWAN) has recently evolved, including LoRa, Sigfox and NB-IoT, hence this book presents the latest updates. A highly detailed guide to performing powerful attack vectors in many hands-on scenarios and defending significant security flaws in your company's infrastructure Key Features Advanced exploitation techniques to breach modern operating systems and complex network devices Learn about Docker breakouts, Active Directory delegation, and CRON jobs Practical use cases to deliver an intelligent endpoint-protected system Book Description It has always been difficult to gain hands-on experience and a comprehensive understanding of advanced penetration testing techniques and vulnerability assessment and management. This book will be your one-stop solution to compromising complex network devices and modern operating systems. This book provides you with advanced penetration testing techniques that will help you exploit databases, web and application servers, switches or routers, Docker, VLAN, VoIP, and VPN. With this book, you will explore exploitation abilities such as offensive PowerShell tools and techniques, CI servers, database exploitation, Active Directory delegation, kernel exploits, cron jobs, VLAN hopping, and Docker breakouts. Moving on, this book will not only walk you through managing vulnerabilities, but will also teach you how to ensure endpoint protection. Toward the end of this book, you will also discover post-exploitation tips, tools, and methodologies to help your organization build an intelligent security system. By the end of this book, you will have mastered the skills and methodologies needed to breach infrastructures and provide complete endpoint protection for your system. What you will learn Exposure to advanced infrastructure penetration testing techniques and methodologies Gain hands-on experience of penetration testing in Linux system vulnerabilities and memory exploitation Understand what it takes to break into enterprise networks Learn to secure the configuration management environment and continuous delivery pipeline Gain an understanding of how to exploit networks and IoT devices Discover real-world, post-exploitation techniques and countermeasures Who this book is for If you are a system administrator, SOC analyst, penetration tester, or a network engineer and want to take your penetration testing skills and security knowledge to the next level, then this book is for you. Some prior experience with penetration testing tools and

knowledge of Linux and Windows command-line syntax is beneficial.

Penetration Testing with Raspberry Pi

CompTIA PenTest+ Certification For Dummies

Practical Industrial Internet of Things Security

Securing the Internet of Things

Develop practical skills to perform pentesting and risk assessment of Microsoft

Azure environments

Pentesting Azure Applications

Target, test, analyze, and report on security vulnerabilities with pen testing Pen Testing is necessary for companies looking to target, test, analyze, and patch the security vulnerabilities from hackers attempting to break into and compromise their organizations data. It takes a person with hacking skills to look for the weaknesses that make an organization susceptible to hacking. Pen Testing For Dummies aims to equip IT enthusiasts at various levels with the basic knowledge of pen testing. It is the go-to book for those who have some IT experience but desire more knowledge of how to gather intelligence on a target, learn the steps for mapping out a test, and discover best practices for analyzing, solving, and reporting on vulnerabilities. The different phases of a pen test from pre-engagement to completion Threat modeling and understanding risk When to apply vulnerability management vs penetration testing Ways to keep your pen testing skills sharp, relevant, and at the top of the game Get ready to gather intelligence, discover the steps for mapping out tests, and analyze and report results! Evade antiviruses and bypass firewalls with the most widely used penetration testing frameworks Key Features Gain insights into the latest antivirus evasion techniques Set up a complete pentesting environment using Metasploit and virtual machines Discover a variety of tools and techniques that can be used with Kali Linux Book Description Penetration testing or ethical hacking is a legal and foolproof way to identify vulnerabilities in your system. With thorough penetration testing, you can secure your system against the majority of threats. This Learning Path starts with an in-depth explanation of what hacking and penetration testing is. You'll gain a deep understanding of classical SQL and command injection flaws, and discover ways to exploit these flaws to secure your system. You'll also learn how to create and customize payloads to evade antivirus software and bypass an organization's defenses. Whether it's exploiting server vulnerabilities and attacking client systems, or compromising mobile phones and installing backdoors, this Learning Path will guide you through all this and more to improve your defense against online attacks. By the end of this Learning Path, you'll have the knowledge and skills you need to invade a system and identify all its vulnerabilities. This Learning Path includes content from the following Packt products: Web Penetration Testing with Kali Linux - Third Edition by Juned Ahmed Ansari and Gilberto Najera-Gutierrez Metasploit Penetration Testing Cookbook - Third Edition by Abhinav Singh , Monika Agarwal, et al What you will learn Build and analyze Metasploit modules in Ruby Integrate Metasploit with other penetration testing tools Use server-side attacks to detect vulnerabilities in web servers and their applications Explore automated attacks such as fuzzing web applications Identify the difference between hacking a web application and network hacking Deploy Metasploit with the Penetration Testing Execution

Standard (PTES) Use MSFvenom to generate payloads and backdoor files, and create shellcode Who this book is for This Learning Path is designed for security professionals, web programmers, and pentesters who want to learn vulnerability exploitation and make the most of the Metasploit framework. Some understanding of penetration testing and Metasploit is required, but basic system administration skills and the ability to read code are a must.

A comprehensive guide to penetration testing cloud services deployed with Microsoft Azure, the popular cloud computing service provider used by companies like Warner Brothers and Apple. Pentesting Azure Applications is a comprehensive guide to penetration testing cloud services deployed in Microsoft Azure, the popular cloud computing service provider used by numerous companies. You'll start by learning how to approach a cloud-focused penetration test and how to obtain the proper permissions to execute it; then, you'll learn to perform reconnaissance on an Azure subscription, gain access to Azure Storage accounts, and dig into Azure's Infrastructure as a Service (IaaS). You'll also learn how to: - Uncover weaknesses in virtual machine settings that enable you to acquire passwords, binaries, code, and settings files - Use PowerShell commands to find IP addresses, administrative users, and resource details - Find security issues related to multi-factor authentication and management certificates - Penetrate networks by enumerating firewall rules - Investigate specialized services like Azure Key Vault, Azure Web Apps, and Azure Automation - View logs and security events to find out when you've been caught Packed with sample pentesting scripts, practical advice for completing security assessments, and tips that explain how companies can configure Azure to foil common attacks, Pentesting Azure Applications is a clear overview of how to effectively perform cloud-focused security tests and provide accurate findings and recommendations.

According to IHS Markit, the number of IoT (Internet of Things) devices will grow to 30.7 billion in 2020, and to 75.4 billion by 2025! IDC Forecasts Worldwide spending on the IoT to reach \$772 Billion in 2018! Whether it is connected automobiles, fitness watches, smart coffee machines, smart locks or even medical equipment such as insulin pumps, IoT is becoming all-pervasive. In the future, there will hardly be any aspect of our lives that IoT will not touch one way or the other. Bluetooth Low Energy (BLE) is one of the popular radio protocols used by many IoT devices. As the footprint of IoT devices has increased, so have the attacks on these devices by cyber criminals. Given our increasing dependency on IoT and the increasing number of cyber attacks on these devices, it's intuitive that their security will have a huge implication on safety and security of the digital society that we are a part of! If you wish to acquire hands-on (BLE) IoT penetration testing and securing skills and be a white hat cyber security superstar, this book is for you!

A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world About This Book Learn to design and implement cyber security strategies for your organization Learn to protect cyber-physical systems and utilize forensic data analysis to beat vulnerabilities in your IoT ecosystem Learn best practices to secure your data from device to the cloud Gain insight into privacy-enhancing techniques and technologies Who This Book Is For This book targets IT Security Professionals and Security Engineers (including pentesters, security architects and ethical hackers) who would like to ensure security of their organization's data when connected through the IoT. Business analysts and managers will also find it

useful. What You Will Learn Learn how to break down cross-industry barriers by adopting the best practices for IoT deployments Build a rock-solid security program for IoT that is cost-effective and easy to maintain Demystify complex topics such as cryptography, privacy, and penetration testing to improve your security posture See how the selection of individual components can affect the security posture of the entire system Use Systems Security Engineering and Privacy-by-design principles to design a secure IoT ecosystem Get to know how to leverage the burdgening cloud-based systems that will support the IoT into the future. In Detail With the advent of Intenret of Things (IoT), businesses will be faced with defending against new types of threats. The business ecosystem now includes cloud computing infrastructure, mobile and fixed endpoints that open up new attack surfaces, a desire to share information with many stakeholders and a need to take action quickly based on large quantities of collected data. . It therefore becomes critical to ensure that cyber security threats are contained to a minimum when implementing new IoT services and solutions. . The interconnectivity of people, devices, and companies raises stakes to a new level as computing and action become even more mobile, everything becomes connected to the cloud, and infrastructure is strained to securely manage the billions of devices that will connect us all to the IoT. This book shows you how to implement cyber-security solutions, IoT design best practices and risk mitigation methodologies to address device and infrastructure threats to IoT solutions. This book will take readers on a journey that begins with understanding the IoT and how it can be applied in various industries, goes on to describe the security challenges associated with the IoT, and then provides a set of guidelines to architect and deploy a secure IoT in your Enterprise. The book will showcase how the IoT is implemented in early-adopting industries and describe how lessons can be learned and shared across diverse industries to support a secure IoT. Style and approach This book aims to educate readers on key areas in IoT security. It walks readers through engaging with security challenges and then provides answers on how to successfully manage IoT security and build a safe infrastructure for smart devices. After reading this book, you will understand the true potential of tools and solutions in order to build real-time security intelligence on IoT networks.

A practitioner's guide to securing connected industries

Defend your systems from methodized and proficient attackers

LPWAN Technologies for IoT and M2M Applications

Effective techniques to secure your Windows, Linux, IoT, and cloud infrastructure Hackable

How to Do Application Security Right

Improving your Penetration Testing Skills

The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more.

Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive

Read PDF IoT Penetration Testing Cookbook: Identify Vulnerabilities And Secure Your Smart Devices

reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to:

- Write a DICOM service scanner as an NSE module
- Hack a microcontroller through the UART and SWD interfaces
- Reverse engineer firmware and analyze mobile companion apps
- Develop an NFC fuzzer using Proxmark3
- Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill

The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things

REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

Penetration Testing

Penetration Testing Essentials

Practical Internet of Things Security

Kali Linux Penetration Testing Bible

Spy on and protect vulnerable ecosystems using the power of Kali Linux for pentesting on the go