Wireshark Labs Solutions

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide
Fundamentals of Communications and Networking with Cloud Labs Access
Applied Networking Labs
Learn Wireshark
Wireshark Certified Network Analyst Exam Prep Guide (Second Edition)
A Practical Guide to Ubuntu Linux
101 Labs - Comptia Network+
Embedded Software for the IoT
Wireshark® Workbook 1
Network Security, Firewalls, and VPNs
Wireshark 101
Network Analysis
Wireshark for Security Professionals
Penetration Testing
101 Labs - IP Subnetting
Build Your Own Cybersecurity Testing Lab: Low-cost Solutions for Testing in Virtual and Cloud-based Environments
The DevOps Handbook
Wireshark Network Analysis
Fundamentals of Communications and Networking
Day One Junos Tips, Techniques, and Templates
Network Security, Firewalls and VPNs
Mastering Wireshark 2.6
Practical Packet Analysis
Implementing and Administering Cisco Solutions: 200-301 CCNA Exam Guide
Wireshark Workbook 1
CompTIA Security+ SY0-501 Cert Guide
Computer Networking
101 Labs - Cisco CCNA
The Network Security Test Lab
CCNA Data Center - Introducing Cisco Data Center Networking Study Guide
Packet Guide to Core Network Protocols
Packet Guide to Routing and Switching
Practical Malware Analysis
Computer Networking: A Top-Down Approach Featuring the Internet, 3/e
Day One Routing in Fat Trees
Learn Ethical Hacking from Scratch
Practical Security Automation and Testing
Wireshark for Security Professionals
SEED Labs
MITRE Systems Engineering Guide

NICOLE MAREN

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide Lightning Source Incorporated
Your one stop guide to automating infrastructure security using DevOps and DevSecOps Key FeaturesSecure and automate techniques to protect web, mobile or cloud servicesAutomate secure code inspection in C++, Java, Python, and JavaScriptIntegrate security testing with automation frameworks like fuzz, BDD, Selenium and Robot FrameworkBook Description Security automation is the automatic handling of software security assessments tasks. This book helps you to build your security automation framework to scan for vulnerabilities without human intervention. This book will teach you to adopt security automation techniques to continuously improve your entire software development and security testing. You will learn to use open source tools and techniques to integrate security testing tools directly into your CI/CD framework. With this book, you will see how to implement security inspection at every layer, such as secure code inspection, fuzz testing, Rest API, privacy, infrastructure security, and web UI testing. With the help of practical examples, this book will teach you to implement the combination of automation and Security in DevOps. You will learn about the integration of security testing results for an overall security status for projects. By the end of this book, you will be confident implementing automation security in all layers of your software development stages and will be able to build your own in-house security automation platform throughout your mobile and cloud releases. What you will learnAutomate secure code inspection with open source tools and effective secure code scanning suggestionsApply security testing tools and automation frameworks to identify security vulnerabilities in web, mobile and cloud servicesIntegrate security testing tools such as OWASP ZAP, NMAP, SSLyze, SQLMap, and OpenSCAPImplement automation testing techniques with Selenium, JMeter, Robot Framework, Gauntlt, BDD, DDT, and Python unittestExecute security testing of a Rest API Implement web application security with open source tools and script templates for CI/CD integrationIntegrate various types of security testing tool results from a single project into one dashboardWho this book is for The book is for software developers, architects, testers and QA engineers who are looking to leverage automated security testing techniques.
Fundamentals of Communications and Networking with Cloud Labs Access IT Revolution
Instructor manual (for instructors only)
Applied Networking Labs Springer
Wireshark is the world's most popular network analyzer solution. Used for network troubleshooting, forensics, optimization and more, Wireshark is considered one of the most successful open source projects of all time. Laura Chappell has been involved in the Wireshark project since its infancy (when it was called Ethereal) and is considered the foremost authority on network protocol analysis and forensics using Wireshark. This book consists of 16 labs and is based on the format Laura introduced to trade show audiences over ten years ago through her highly acclaimed "Packet Challenges." This book gives you a chance to test your

knowledge of Wireshark and TCP/IP communications analysis by posing a series of questions related to a trace file and then providing Laura's highly detailed step-by-step instructions showing how Laura arrived at the answers to the labs. Book trace files and blank Answer Sheets can be downloaded from this book's supplement page (see https: //www.chappell-university.com/books). Lab 1: Wireshark Warm-Up Objective: Get Comfortable with the Lab Process. Completion of this lab requires many of the skills you will use throughout this lab book. If you are a bit shaky on any answer, take time when reviewing the answers to this lab to ensure you have mastered the necessary skill(s). Lab 2: Proxy Problem Objective: Examine issues that relate to a web proxy connection problem. Lab 3: HTTP vs. HTTPS Objective: Analyze and compare HTTP and HTTPS communications and errors using inclusion and field existence filters. Lab 4: TCP SYN Analysis Objective: Filter on and analyze TCP SYN and SYN/ACK packets to determine the capabilities of TCP peers and their connections. Lab 5: TCP SEQ/ACK Analysis Objective: Examine and analyze TCP sequence and acknowledgment numbering and Wireshark's interpretation of non-sequential numbering patterns. Lab 6: You're Out of Order! Objective: Examine Wireshark's process of distinguishing between out-of-order packets and retransmissions and identify mis-identifications. Lab 7: Sky High Objective: Examine and analyze traffic captured as a host was redirected to a malicious site. Lab 8: DNS Warm-Up Objective: Examine and analyze DNS name resolution traffic that contains canonical name and multiple IP address responses. Lab 9: Hacker Watch Objective: Analyze TCP connections and FTP command and data channels between hosts. Lab 10: Timing is Everything Objective: Analyze and compare path latency, name resolution, and server response times. Lab 11: The News Objective: Analyze capture location, path latency, response times, and keepalive intervals between an HTTP client and server. Lab 12: Selective ACKs Objective: Analyze the process of establishing Selective acknowledgment (SACK) and using SACK during packet loss recovery. Lab 13: Just DNS Objective: Analyze, compare, and contrast various DNS queries and responses to identify errors, cache times, and CNAME (alias) information. Lab 14: Movie Time Objective: Use various display filter types, including regular expressions (regex), to analyze HTTP redirections, end-of-field values, object download times, errors, response times and more. Lab 15: Crafty Objective: Practice your display filter skills using "contains" operators, ASCII filters, and inclusion/exclusion filters, while analyzing TCP and HTTP performance parameters. Lab 16: Pattern Recognition Objective: Focus on TCP conversations and endpoints while analyzing TCP sequence numbers, Window Scaling, keep-alive, and Selective Acknowledgment capabilities.

Learn Wireshark Pearson Education India

Follow along, hands-on labs to prepare you for the Cisco CCNA 200-301 exam.

Wireshark Certified Network Analyst Exam Prep Guide (Second Edition) John Wiley & Sons

101 Labs - Book Series Experts agree that we retain only 10% of what we read but 90% of what we do. Perhaps this explains why the global pass rate for most IT exams is a ghastly 40%. This is

where the 101 Labs book series can help. We are revolutionizing how IT people train for their exams and the real world with our Learn - By - Doing teaching method. 101 Labs' mission is to turn you into an IT expert by doing instead of reading. Using free software and free trials, our experts take you by the hand and walk you through every aspect of the protocols and technologies you will encounter in your IT career. We share our configuration tips and tricks with you as well as how to avoid the common mistakes many novice engineers make, which can quickly become career-ending. 101 Labs - IP Subnetting Subnetting is one of the toughest subjects for IT students and engineers to understand. You have to master binary math, hexadecimal numbering systems and address classes. You must determine which IP address is in which subnet and which subnet mask will provide you with the requisite number of subnet and hosts-per-subnet. You will often have to do this during a crisis on a live network with your boss, customers and other engineers watching you! Subnetting questions form around 9% of your score in exams such as CompTIA Network+ and the Cisco CCNA. If you work in IT, you will be expected to understand how to subnet and troubleshoot subnetting problems. You will also be expected to be able to allocate IP addressing schemes to various departments in your organization. For job interviews you can expect to be grilled on subnetting problems by senior engineers. 101 Labs - IP Subnetting shows you how to answer any subnetting or network design problem using a simple Cheat Chart. All you need to do is tick the boxes and you get the answer, usually in under 60 seconds. We show you how to subnet IPv6 networks, work out wildcard masks for your firewalls, NAT, routing and access lists. We also show you how to summarize routes for your routing advertisements. All answers and working out are provided. You finish by drilling 33 exam style questions so by the end of the course, you will be the go-to subnetting expert at work. Please use the free resources at www.101labs.net/resources which will help you with the labs. About the Author Paul Browning left behind a career in law enforcement in 2000 and started an IT consulting and training company. He's written over 15 best selling IT books and through his books, classroom courses, and websites he's trained tens of thousands of people from all walks of life. He's spent the last 16 years dedicated to training and teaching IT students from all walks of life to pass their exams and enjoy a rewarding career.

A Practical Guide to Ubuntu Linux Packt Publishing Ltd

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, Practical Malware Analysis will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to: –Set up a safe virtual environment to analyze malware –Quickly extract network signatures and host-based indicators –Use key analysis tools like IDA Pro, OllyDbg, and WinDbg –Overcome malware tricks like obfuscation, anti-disassembly, anti-

debugging, and anti-virtual machine techniques –Use your newfound knowledge of Windows internals for malware analysis –Develop a methodology for unpacking malware and get practical experience with five of the most popular packers –Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You'll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're making a living as a malware analyst, you'll find what you need to succeed in Practical Malware Analysis.

101 Labs - Comptia Network+ Jones & Bartlett Publishers

Based on over 20 years of analyzing networks and teaching key analysis skills, this Second Edition covers the key features and functions of Wireshark version 2. This book includes 46 Labs and end-of-chapter Challenges to help you master Wireshark for troubleshooting, security, optimization, application analysis, and more.

Embedded Software for the IoT Pearson IT Certification

Publisher's Note: Products purchased from Third Party sellers are not guaranteed by the publisher for quality, authenticity, or access to any online entitlements included with the product.

Manage your own robust, inexpensive cybersecurity testing environment This hands-on guide shows clearly how to administer an effective cybersecurity testing lab using affordable technologies and cloud resources. Build Your Own Cybersecurity Testing Lab: Low-cost Solutions for Testing in Virtual and Cloud-based Environments fully explains multiple techniques for developing lab systems, including the use of Infrastructure-as-Code, meaning you can write programs to create your labs quickly, without manual steps that could lead to costly and frustrating mistakes. Written by a seasoned IT security professional and academic, this book offers complete coverage of cloud and virtual environments as well as physical networks and automation. Included with the book is access to videos that demystify difficult concepts. Inside, you will discover how to: • Gather network requirements and build your cybersecurity testing lab • Set up virtual machines and physical systems from inexpensive components • Select and configure the necessary operating systems • Gain remote access through SSH, RDP, and other remote access protocols • Efficiently isolate subnets with physical switches, routers, and VLANs • Analyze the vulnerabilities and challenges of cloud-based infrastructures • Handle implementation of systems on Amazon Web Services, Microsoft Azure, and Google Cloud Engine • Maximize consistency and repeatability using the latest automation tools

Wireshark® Workbook 1 Pearson Higher Ed

101 Labs - Book Series Experts agree that we retain only 10% of what we read but 90% of what we do. Perhaps this explains why the global pass rate for most IT exams is a ghastly 40%. This is

where the 101 Labs book series can help. We are revolutionizing how IT people train for their exams and the real world with our Learn - By - Doing teaching method. 101 Labs' mission is to turn you into an IT expert by doing instead of reading. Using free software and free trials, our experts take you by the hand and walk you through every aspect of the protocols and technologies you will encounter in your IT career. We share our configuration tips and tricks with you as well as how to avoid the common mistakes many novice engineers make, which can quickly become career-ending. 101 Labs - CompTIA Network] This book is designed to help you pass the new N10-007 exam. It now features Performance-based questions (PBQs). These questions test your configuration and troubleshooting skills and add a new level of complexity to the exam. The only way to answer these types of questions is to have hands-on experience with the protocols and technology listed in the exam syllabus. The Network+ exam is probably the most useful exam in the IT industry. It equips you with all the necessary knowledge you need in order to work with other IT professionals and work in the IT industry. You learn TCP/IP, security, networking protocols and standards, best practices, subnetting and IP addressing, IPv6, troubleshooting tools and software, security, wireless, routing protocol basics, and much more. CompTIA presumes around 9-12 months of on-the-job experience for all of its exams, but of course, most of the students who take the exam don't have this. Even if they are working in IT roles, such as in helpdesk or server support, they will have been exposed to only a tiny number of the skills tested in the exam. Doing all the labs in this book will give you that experience. Please use the free resources at www.101labs.net/resources which will help you with the labs. About the Author Paul Browning left behind a career in law enforcement in 2000 and started an IT consulting and training company. He's written over 15 best selling IT books and through his books, classroom courses, and websites he's trained tens of thousands of people from all walks of life. He's spent the last 16 years dedicated to training and teaching IT students from all walks of life to pass their exams and enjoy a rewarding career.

Network Security, Firewalls, and VPNs Jones & Bartlett Publishers

"Wireshark is the world's foremost and most widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level. Wireshark deals with the second to the seventh layers of network protocols, and the analysis made is presented in a human-readable form. It is used for network troubleshooting, analysis, software, and communications protocol development. This course starts setting up a Wireshark lab in the Windows and Linux operating systems. We dive into the overall process of packet capturing and Wireshark filters. Then, we introduce tshark, a command line-version of Wireshark, and we learn about various tshark commands. Later, we are introduced to various types of network cyber attack and essential remedies. We also go through an array of techniques to monitor and secure these attacks using Wireshark. Lastly, we cover network troubleshooting using Wireshark. Towards the end of the course, you'll use Wireshark efficiently to find primary sources of network

performance problems and also different ways to secure networks."--Resource description page.

Wireshark 101 No Starch Press

This is the eBook version of the print title. Note that the eBook may not provide access to the practice test software that accompanies the print book. Access to the companion files are available through product registration at Pearson IT Certification, or see the instructions in the back pages of your eBook. Learn, prepare, and practice for CompTIA Security+ SY0-501 exam success with this CompTIA approved Cert Guide from Pearson IT Certification, a leader in IT certification learning and a CompTIA Authorized Platinum Partner. · Master CompTIA Security+ SY0-501 exam topics · Assess your knowledge with chapter-ending quizzes · Review key concepts with exam preparation tasks · Practice with realistic exam questions CompTIA Security+ SY0-501 Cert Guide is a best-of-breed exam study guide. Best-selling author and expert instructor David L. Prowse shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test-preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending chapter review activities help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. Well regarded for its level of detail, assessment features, and challenging review questions and exercises, this CompTIA approved study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The CompTIA approved study guide helps you master all the topics on the Security+ exam, including · Core computer system security · OS hardening and virtualization · Application security · Network design elements · Networking ports, protocols, and threats · Network perimeter security · Physical security and authentication models · Access control · Vulnerability and risk assessment · Monitoring and auditing · Cryptography, including PKI · Redundancy and disaster recovery · Social Engineering · Policies and procedures

Network Analysis Walter de Gruyter GmbH & Co KG

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 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.

Wireshark for Security Professionals "O'Reilly Media, Inc."

Today's networks are required to support an increasing array of real-time communication methods. Video chat, real-time messaging, and always-connected resources put demands on networks that were previously unimagined. The Second Edition of Fundamentals of Communications and Networking helps readers better understand today's networks and the way they support the evolving requirements of different types of organizations. It discusses the critical issues of designing a network that will meet an organization's performance needs and discusses how businesses use networks to solve business problems. Using numerous examples and exercises, this text incorporates hands-on activities to prepare readers to fully understand and design modern networks and their requirements. Key Features of the Second Edition: - Introduces network basics by describing how networks work - Discusses how networks support the increasing demands of advanced communications - Illustrates how to map the right technology to an organization's needs and business goals - Outlines how businesses use networks to solve business problems, both technically and operationally.

Penetration Testing John Wiley & Sons

"Network analysis is the process of listening to and analyzing network traffic. Network analysis offers an insight into network communications to identify performance problems, locate security breaches, analyze application behavior, and perform capacity planning. Network analysis (aka "protocol analysis") is a process used by IT professionals who are responsible for network performance and security." -- p. 2.

101 Labs - IP Subnetting "O'Reilly Media, Inc."

Learn how to hack systems like black hat hackers and secure them like security experts Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to secure systems from hackers Book Description This book starts with the basics of ethical hacking, how to practice hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking, where you will see how to test the security of wired and wireless networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks. You will also get the hang of post-exploitation techniques, including remotely controlling and interacting with the systems that you compromised. Towards the end of the

book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the different fields and types of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how to hack and test the security of systems like professional hackers and security experts.

Build Your Own Cybersecurity Testing Lab: Low-cost Solutions for Testing in Virtual and Cloud-based Environments Laura Chappell University

The Most Complete, Easy-to-Follow Guide to Ubuntu Linux The #1 Ubuntu server resource, fully updated for Ubuntu 10.4 (Lucid Lynx)-the Long Term Support (LTS) release many companies will rely on for years! Updated JumpStarts help you set up Samba, Apache, Mail, FTP, NIS, OpenSSH, DNS, and other complex servers in minutes Hundreds of up-to-date examples, plus comprehensive indexes that deliver instant access to answers you can trust Mark Sobell's A Practical Guide to Ubuntu Linux®, Third Edition, is the most thorough and up-to-date reference to installing, configuring, and working with Ubuntu, and also offers comprehensive coverage of servers--critical for anybody interested in unleashing the full power of Ubuntu. This edition has been fully updated for Ubuntu 10.04 (Lucid Lynx), a milestone Long Term Support (LTS) release, which Canonical will support on desktops until 2013 and on servers until 2015. Sobell walks you through every essential feature and technique, from installing Ubuntu to working with GNOME, Samba, exim4, Apache, DNS, NIS, LDAP, g ufw, firestarter, iptables, even Perl scripting. His exceptionally clear explanations demystify everything from networking to security. You'll find full chapters on running Ubuntu from the command line and desktop (GUI), administrating systems, setting up networks and Internet servers, and much more. Fully updated JumpStart sections help you get complex servers running--often in as little as five minutes. Sobell draws on his immense Linux knowledge to explain both the "hows" and the "whys" of Ubuntu. He's taught hundreds of thousands of readers and never forgets what it's like to be new to Linux. Whether you're a user, administrator, or programmer, you'll find everything you need here--now, and for many years to come. The world's most practical Ubuntu Linux book is now even more useful! This book delivers Hundreds of easy-to-use Ubuntu examples Important networking coverage, including DNS, NFS, and Cacti Coverage of crucial Ubuntu topics such as sudo and the Upstart init daemon More detailed, usable coverage of Internet server configuration, including

Apache (Web) and exim4 (email) servers State-of-the-art security techniques, including up-to-date firewall setup techniques using gufw and iptables, and a full chapter on OpenSSH A complete introduction to Perl scripting for automated administration Deeper coverage of essential admin tasks-from managing users to CUPS printing, configuring LANs to building a kernel Complete instructions on keeping Ubuntu systems up-to-date using aptitude, Synaptic, and the Software Sources window And much more...including a 500+ term glossary Includes DVD! Get the full version of Lucid Lynx, the latest Ubuntu LTS release!

The DevOps Handbook Independently Published

Go beyond layer 2 broadcast domains with this in-depth tour of advanced link and internetwork layer protocols, and learn how they enable you to expand to larger topologies. An ideal follow-up to Packet Guide to Core Network Protocols, this concise guide dissects several of these protocols to explain their structure and operation. This isn't a book on packet theory. Author Bruce Hartpence built topologies in a lab as he wrote this guide, and each chapter includes several packet captures. You'll learn about protocol classification, static vs. dynamic topologies, and reasons for installing a particular route. This guide covers: Host routing—Process a routing table and learn how traffic starts out across a network Static routing—Build router routing tables and understand how forwarding decisions are made and processed Spanning Tree Protocol—Learn how this protocol is an integral part of every network containing switches Virtual Local Area Networks—Use VLANs to address the limitations of layer 2 networks Trunking—Get an indepth look at VLAN tagging and the 802.1Q protocol Routing Information Protocol—Understand how this distance vector protocol works in small, modern communication networks Open Shortest Path First—Discover why convergence times of OSPF and other link state protocols are improved over distance vectors

Wireshark Network Analysis John Wiley & Sons

This book is intended to provide practice quiz questions based on the thirty-three areas of study defined for the Wireshark Certified Network AnalystT Exam. This Official Exam Prep Guide offers a companion to Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide (Second Edition).

Fundamentals of Communications and Networking Jones & Bartlett Publishers

Master Wireshark to solve real-world security problems If you don't already use Wireshark for a wide range of information security tasks, you will after this book. Mature and powerful, Wireshark is commonly used to find root cause of challenging network issues. This book extends that power to information security professionals, complete with a downloadable, virtual lab environment. Wireshark for Security Professionals covers both offensive and defensive concepts that can be applied to essentially any InfoSec role. Whether into network security, malware analysis, intrusion detection, or penetration testing, this book demonstrates Wireshark through relevant and useful examples. Master Wireshark through both lab scenarios and exercises. Early in the book, a virtual lab environment is provided for the purpose of getting hands-on experience with Wireshark.

Wireshark is combined with two popular platforms: Kali, the security-focused Linux distribution, and the Metasploit Framework, the open-source framework for security testing. Lab-based virtual systems generate network traffic for analysis, investigation and demonstration. In addition to following along with the labs you will be challenged with end-of-chapter exercises to expand on covered material. Lastly, this book explores Wireshark with Lua, the light-weight programming language. Lua allows you to extend and customize Wireshark's features for your needs as a security professional. Lua source code is available both in the book and online. Lua code and lab source code are available online through GitHub, which the book also introduces. The book's final two chapters greatly draw on Lua and TShark, the command-line interface of Wireshark. By the end of the book you will gain the following: Master the basics of Wireshark Explore the virtual w4sp-lab environment that mimics a real-world network Gain experience using the Debian-based Kali OS among other systems Understand the technical details behind network attacks Execute exploitation and grasp offensive and defensive activities, exploring them through Wireshark Employ Lua to extend Wireshark features and create useful scripts To sum up, the book content, labs and online material, coupled with many referenced sources of PCAP traces, together present a dynamic and robust manual for information security professionals seeking to leverage Wireshark.

Day One Junos Tips, Techniques, and Templates John Wiley & Sons Provides information on ways to use Wireshark to capture and analyze packets, covering such topics as building customized capture and display filters, graphing traffic patterns, and building statistics and reports.