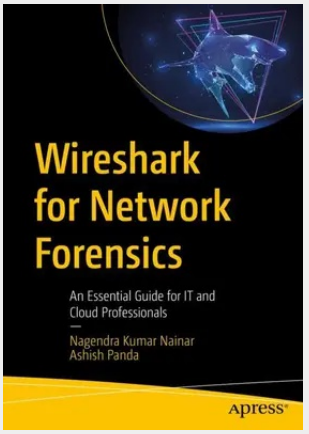
Nainar / Panda

Wireshark for Network Forensics

An Essential Guide for IT and Cloud Professionals



64,19 €
59,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9781484290002
Medium: Buch
ISBN: 978-1-4842-9000-2
Verlag: Apress
Erscheinungstermin: 31.12.2022
Sprache(n): Englisch
Auflage: 1. Auflage 2022
Produktform: Kartoniert
Gewicht: 554 g
Seiten: 271
Format (B x H): 178 x 254 mm

With the advent of emerging and complex technologies, traffic capture and analysis play an integral part in the overall IT operation. This book outlines the rich set of advanced features and capabilities of the Wireshark tool, considered by many to be the de-facto Swiss army knife for IT operational activities involving traffic analysis. This open-source tool is available as CLI or GUI. It is designed to capture using different modes, and to leverage the community developed and integrated features, such as filter-based analysis or traffic flow graph view.

You'll start by reviewing the basics of Wireshark, and then examine the details of capturing and analyzing secured application traffic such as SecureDNS, HTTPS, and IPSec. You'll then look closely at the control plane and data plane capture, and study the analysis of wireless technology traffic such as 802.11, which is the common access technology currently used, along with Bluetooth. You'll also learn waysto identify network attacks, malware, covert communications, perform security incident post mortems, and ways to prevent the same.

The book further explains the capture and analysis of secure multimedia traffic, which constitutes around 70% of all overall internet traffic. *Wireshark for Network Forensics* provides a unique look at cloud and cloud-native architecture-based traffic capture in Kubernetes, Docker-based, AWS, and GCP environments.

What You'll Learn

- Review Wireshark analysis and network forensics
- Study traffic capture and its analytics from mobile devices
- Analyze various access technology and cloud traffic
- Write your own dissector for any new or proprietary packet formats
- Capture secured application traffic for analysis

Who This Book Is For

IT Professionals, Cloud Architects, Infrastructure Administrators, and Network/Cloud Operators

With the advent of emerging and complex technologies, traffic capture and analysis play an integral part in the overall IT operation. This book outlines the rich set of advanced features and capabilities of the Wireshark tool, considered by many to be the de-facto Swiss army knife for IT operational activities involving traffic analysis. This open-source tool is available as CLI or GUI. It is designed to capture using different modes, and to leverage the community developed and integrated features, such as filter-based analysis or traffic flow graph view. You'll start by reviewing the basics of Wireshark, and then examine the details of capturing and analyzing secured application traffic such as SecureDNS, HTTPS, and IPSec. You'll then look closely at the control plane and data plane capture, and study the analysis of wireless technology traffic such as 802.11, which is the common access technology currently used, along with Bluetooth. You'll also learn waysto identify network attacks, malware, covert communications, perform security incident post mortems, and ways to prevent the same. The book further explains the capture and analysis of secure multimedia traffic, which constitutes around 70% of all overall internet traffic. Wireshark for Network Forensics provides a unique look at cloud and cloud-native architecture-based traffic capture in Kubernetes, Docker-based, AWS, and GCP environments. What You'll LearnReview Wireshark analysis and network forensicsStudy traffic capture and its analytics from mobile devicesAnalyze various access technology and cloud trafficWrite your own dissector for any new or proprietary packet formatsCapture secured application traffic for analysisWho This Book Is ForIT

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)