1. Record Nr. UNINA9910698650103321

Autore	Cardwell Kevin
Titolo	Tactical Wireshark : A Deep Dive into Intrusion Analysis, Malware Incidents, and Extraction of Forensic Evidence / / by Kevin Cardwell
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2023
ISBN	9781484292914 148429291X
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (XV, 462 p. 490 illus., 250 illus. in color.)
Disciplina	929.605
Soggetti	Open source software Computer science Open Source Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Chapter 01: Customization of the Wireshark Interface -- Chapter 02: Capturing Network Traffic -- Chapter 03: Interpreting Network Protocols -- Chapter 04: Analysis of Network Attacks -- Chapter 05: Effective Network Traffic Filtering -- Chapter 06: Advanced Features of Wireshark -- Chapter 07: Scripting and interacting with Wireshark -- Chapter 08: Basic Malware Traffic Analysis -- Chapter 09: Analyzing Encoding, Obfuscated and ICS Malware Traffic -- Chapter 10: Dynamic Malware Network Activities -- Chapter 11: Extractions of Forensic Data with Wireshark -- Chapter 12: Network Traffic Forensics -- Chapter 13: Conclusion.
Sommario/riassunto	Take a systematic approach at identifying intrusions that range from the most basic to the most sophisticated, using Wireshark, an open source protocol analyzer. This book will show you how to effectively manipulate and monitor different conversations and perform statistical analysis of these conversations to identify the IP and TCP information of interest. Next, you'll be walked through a review of the different methods malware uses, from inception through the spread across and compromise of a network of machines. The process from the initial “click” through intrusion, the characteristics of Command and Control

(C2), and the different types of lateral movement will be detailed at the packet level. In the final part of the book, you'll explore the network capture file and identification of data for a potential forensics extraction, including inherent capabilities for the extraction of objects such as file data and other corresponding components in support of a forensics investigation. After completing this book, you will have a complete understanding of the process of carving files from raw PCAP data within the Wireshark tool. You will: Use Wireshark to identify intrusions into a network Exercise methods to uncover network data even when it is in encrypted form Analyze malware Command and Control (C2) communications and identify IOCs Extract data in a forensically sound manner to support investigations Leverage capture file statistics to reconstruct network events.