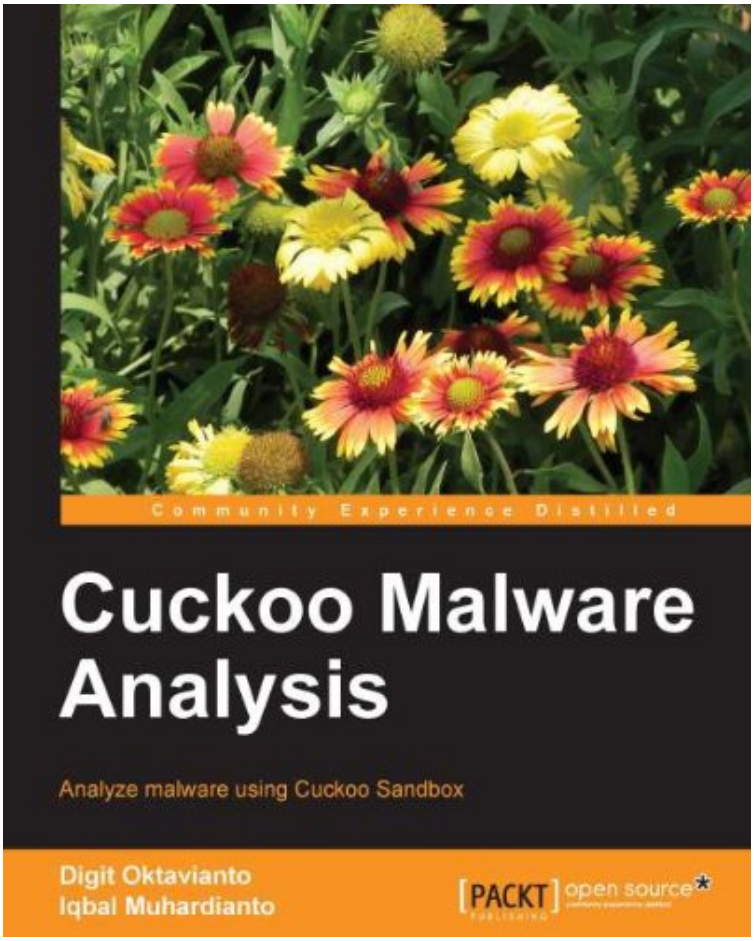
Cuckoo Malware Analysis

Von Digit Oktavianto, Iqbal Muhardianto
*ebooks | Download PDF | *ePub | DOC | audiobook*



Produktinformation -Verkaufsrang: #865669 in eBooksVerffentlicht am: 2013-10-16Erscheinungsdatum: 2013-10-16File Name: B00FXS48SE | File size: 26.Mb

Von Digit Oktavianto, Iqbal Muhardianto : Cuckoo Malware Analysis before purchasing it in order to gage whether or not it would be worth my time, and all praised Cuckoo Malware Analysis:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. A nice cookbook for rookies in malware analysisVon Frank BoldewinImagine you have the need to analyse malware urgently, but don't want to upload the binary somewhere on the internet, as you want to keep it private for now. Then the malware analysis system Cuckoo is the right choice. Especially rookies in malware analysis will really like the capabilities and features Cuckoo provides. This book starts with an overview about the architecture, followed by explaining how to install and configure Cuckoo step by step and how the different types of malware, e.g. PDF, MSOffice, PE-Binaries and so forth are being submitted. In addition the authors give tips and tricks how to harden Cuckoo against VM detection and how to graphically represent the analysed data in Maltego.

KurzbeschreibungIn DetailCuckoo Sandbox is a leading open source automated malware analysis system. This means that you can throw any suspicious file at it and, in a matter of seconds, Cuckoo will provide you with some detailed results outlining what said file did when executed inside an isolated environment.Cuckoo Malware Analysis is a hands-on guide that will provide you with everything you need to know to use Cuckoo Sandbox with added tools like Volatility, Yara, Cuckooforcanari, Cuckoomx, Radare, and Bokken, which will help you to learn malware analysis in an easier and more efficient way.Cuckoo Malware Analysis will cover basic theories in sandboxing, automating malware analysis, and how to prepare a safe environment lab for malware analysis. You will get acquainted with Cuckoo Sandbox architecture and learn how to install Cuckoo Sandbox, troubleshoot the problems after installation, submit malware samples, and also analyze PDF files, URLs, and binary files. This book also covers memory forensics using the memory dump feature, additional memory forensics using Volatility, viewing result analyses using the Cuckoo analysis package, and analyzing APT attacks using Cuckoo Sandbox, Volatility, and Yara.Finally, you will also learn how to screen Cuckoo Sandbox against VM detection and how to automate the scanning of e-mail attachments with Cuckoo.ApproachThis book is a step-by-step, practical tutorial for analyzing and detecting malware and performing digital investigations. This book features clear and concise guidance in an easily accessible format.Who this book is forCuckoo Malware Analysis is great for anyone who wants to analyze malware through programming, networking, disassembling, forensics, and virtualization. Whether you are new to malware analysis or have some experience, this book will help you get started with Cuckoo Sandbox so you can start analysing malware effectively and efficiently.KurzbeschreibungIn DetailCuckoo Sandbox is a leading open source automated malware analysis system. This means that you can throw any suspicious file at it and, in a matter of seconds, Cuckoo will provide you with some detailed results outlining what said file did when executed inside an isolated environment.Cuckoo Malware Analysis is a hands-on guide that will provide you with everything you need to know to use Cuckoo Sandbox with added tools like Volatility, Yara, Cuckooforcanari, Cuckoomx, Radare, and Bokken, which will help you to learn malware analysis in an easier and more efficient way.Cuckoo Malware Analysis will cover basic theories in sandboxing, automating malware analysis, and how to prepare a safe environment lab for malware analysis. You will get acquainted with Cuckoo Sandbox architecture and learn how to install Cuckoo Sandbox, troubleshoot the problems after installation, submit malware samples, and also analyze PDF files, URLs, and binary files. This book also covers memory forensics using the memory dump feature, additional memory forensics using Volatility, viewing result analyses using the Cuckoo analysis package, and analyzing APT attacks using Cuckoo Sandbox, Volatility, and Yara.Finally, you will also learn how to screen Cuckoo Sandbox against VM detection and how to automate the scanning of e-mail attachments with Cuckoo.ApproachThis book is a step-by-step, practical tutorial for analyzing and detecting malware and performing digital investigations. This book features clear and concise guidance in an easily accessible format.Who this book is forCuckoo Malware Analysis is great for anyone who wants to analyze malware through programming, networking, disassembling, forensics, and virtualization. Whether you are new to malware analysis or have some experience, this book will help you get started with Cuckoo Sandbox so you can start analysing malware effectively and efficiently.ber den Autor und weitere MitwirkendeDigit Oktavianto Digit Oktavianto is an IT security professional and system administrator with experience in the Linux server, network security, Security Information and Event Management (SIEM), vulnerability assesment, penetration testing, intrusion analysis, incident response and incident handling, security hardening, PCI-DSS, and system administration. He has good experience in Managed Security Services (MSS) projects, Security Operation Centre, operating and maintaining SIEM tools, configuring and setup of IDS/IPS, Firewall, Antivirus, Operating Systems, and Applications. He works as an information security analyst in Noosc Global, a security consultant firm based in Indonesia. Currently, he holds CEH and GIAC Incident Handler certifications. He is very enthusiastic and has a good passion in malware analysis as his main interest for research. This book is the first book that he has written, and he plans to write more about malware analysis and incident response books.Iqbal Muhardianto Iqbal Muhardianto is a security enthusiast and he is working in the Ministry of Foreign Affairs of the Republic of Indonesia. He loves breaking things apart just to know how it works. In his computer learning career, he first started with learning MS-DOS and some C programming, after being a System admin, Network Admin, and now he is a IT Security Administrator with some skills in Linux, Windows, Network, SIEM, Malware Analysis, and Pentesting. He currently lives Norway and works as an IT Staff in the Indonesia Embassy in Oslo.