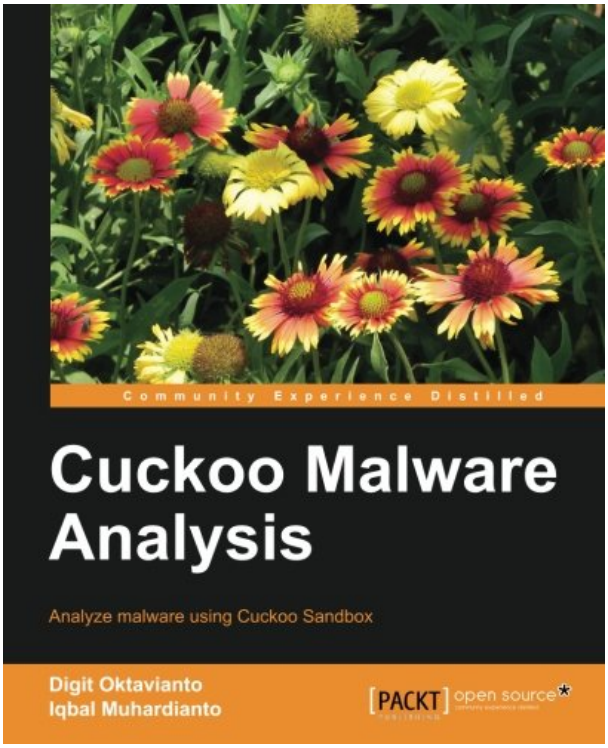
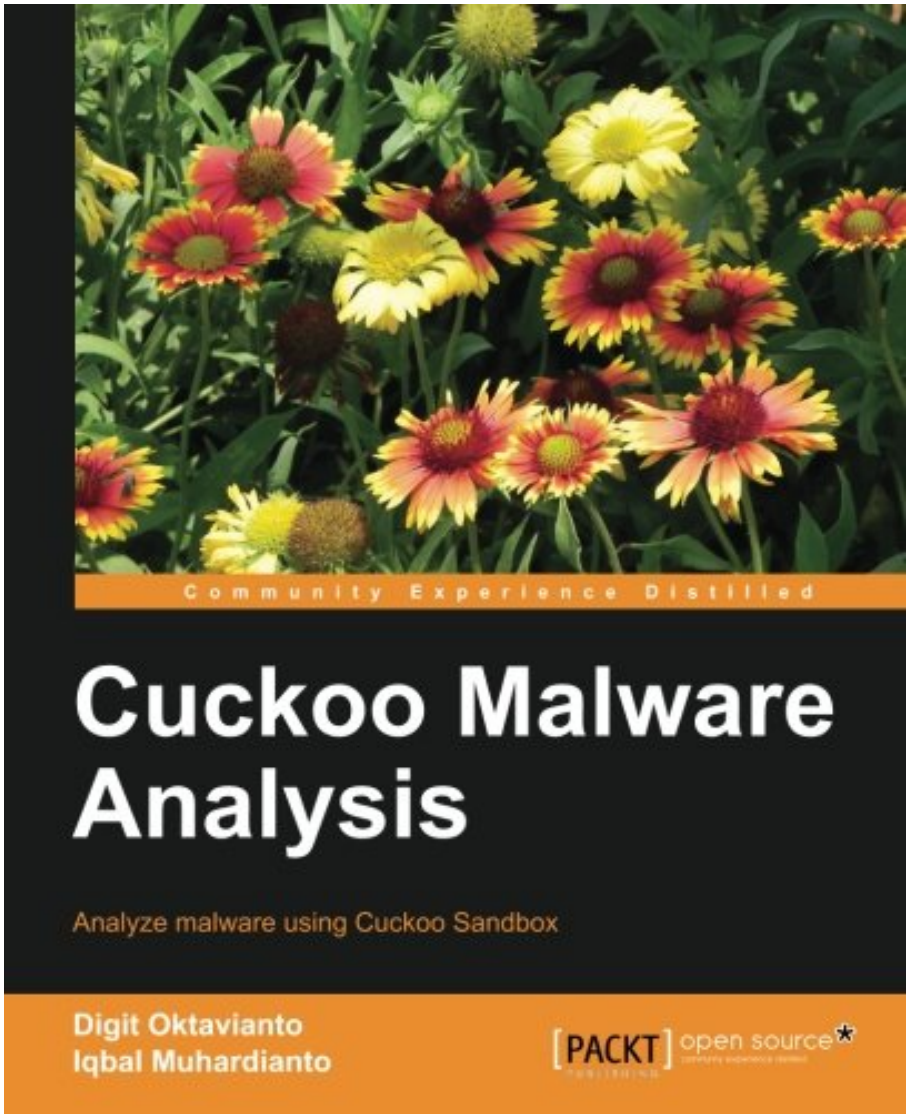
CUCKOO MALWARE ANALYSIS BY DIGIT OKTAVIANTO, IQBAL MUHARDIANTO





CUCKOO MALWARE ANALYSIS BY DIGIT OKTAVIANTO, IQBAL MUHARDIANTO PDF

While the other people in the shop, they are uncertain to discover this Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto straight. It could need more times to go establishment by store. This is why we expect you this site. We will certainly provide the most effective means and also reference to obtain the book Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto Even this is soft data book, it will be convenience to bring Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto any place or save in the house. The difference is that you might not require move the book Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto place to area. You may need only duplicate to the various other gadgets.

About the Author

Digit 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.

CUCKOO MALWARE ANALYSIS BY DIGIT OKTAVIANTO, IQBAL MUHARDIANTO PDF

Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto When creating can change your life, when creating can enhance you by offering much cash, why do not you try it? Are you still extremely confused of where understanding? Do you still have no idea with exactly what you are going to write? Currently, you will certainly need reading Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto A great writer is a great reader at the same time. You could define how you write depending upon what publications to review. This Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto could assist you to fix the problem. It can be one of the ideal resources to create your creating skill.

The benefits to take for checking out the publications *Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto* are concerning improve your life high quality. The life high quality will not simply about the amount of knowledge you will certainly get. Even you read the enjoyable or amusing publications, it will aid you to have improving life quality. Feeling enjoyable will lead you to do something completely. Furthermore, the book Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto will provide you the session to take as a great need to do something. You may not be ineffective when reviewing this publication Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto

Never ever mind if you don't have enough time to head to guide establishment and look for the favourite e-book to check out. Nowadays, the on-line publication Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto is coming to provide convenience of reviewing routine. You may not need to go outside to search guide Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto Searching as well as downloading guide qualify Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto in this write-up will certainly provide you much better remedy. Yeah, online e-book Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto is a sort of electronic publication that you could get in the link download given.

CUCKOO MALWARE ANALYSIS BY DIGIT OKTAVIANTO, IQBAL MUHARDIANTO PDF

Analyze malware using Cuckoo Sandbox

Overview

- Learn how to analyze malware in a straightforward way with minimum technical skills
- Understand the risk of the rise of document-based malware
- Enhance your malware analysis concepts through illustrations, tips and tricks, step-by-step instructions, and practical real-world scenarios

In Detail

Cuckoo 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.

What you will learn from this book

- Get started with automated malware analysis using Cuckoo Sandbox
- Use Cuckoo Sandbox to analyze sample malware
- Analyze output from Cuckoo Sandbox
- Report results with Cuckoo Sandbox in standard form
- Learn tips and tricks to get the most out of your malware analysis results

Approach

This 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 written for

Cuckoo 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.

- Sales Rank: #1750974 in Books
- Published on: 2013-10-16
- Released on: 2013-10-16
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x .32" w x 7.50" l, .56 pounds
- Binding: Paperback
- 142 pages

About the Author

Digit 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.

Most helpful customer reviews

8 of 8 people found the following review helpful.
DONT WASTE YOUR TIME OR MONEY ON THIS BOOK - Use online guides instead
By T. Jones
This book seems like a very rushed product with only thoughts of profit off of a freely shared tool. I plan on writing a more detailed review/complaint to the authors but here are my thoughts:

1) You're better off following the "official" cuckoo configuration guide, which can be found on their webpage, or one of many other freely available guides online. That being said, Chapter 1 of this book (installing cuckoo) is taken almost word for word from the official online guide from the developers of the software. This is a continuing theme throughout the book as most of the other chapters (there's only 5 by the way) are taken from other free sources and can easily be found online.

2) You can't be a complete novice and use solely this book. I'm no Linux/Malware/Programming guru, but I've had plenty of hands on experience with each to make my way. The most difficult part of cuckoo is actually installing the software; between the dependencies, networking and OS you're willing to install malware on, it's a daunting task. Like I said earlier, Ch 1 is about 95% of the online guide. While the online guide is great, it has a few underlying tricks they fail to mention during install and that's ok for a free install guide - not for a published book. I really tried to use this book as my only source to install cuckoo, but I eventually tossed it in favor of the official guide and a few others I found online.

3) Don't expect any new or ground breaking tips. I tried installing cuckoo almost a year ago and that was before I really knew how to handle malware. Now that I've had some experience with it, I was hoping the book at least offered some interesting tips or customizations but once again I was disappointed. The only thing that I could not found somewhere else online was how to configure cuckoo to do PDF reporting. The authors used PDFkit/wkhtmltopdf to generate the reports, so if you know how to install that and know your way around Python, you can easily duplicate the one shining thing I found in this book.

4) There is poor organization throughout the book. It's not uncommon to see the authors reference something as though they have previously talked about it, but in fact it is their first time mentioning it. In some cases it's annoying and in others I think it's down right unacceptable.

5) To me, there are too many operational issues. First of all, they tell you to go to the publishers webpage to download the malware and codes. You go to publishers website and you need to enter in your email address (I don't know about you, but I don't freely give that out). This is for what I believe to be the "code". If you scroll past the email bar, you'll see another link that gives you "updated samples". This is just a blog webpage the authors set up to post information. Why not include this webpage in the book instead of the publishers page?? Worse part is, the malware samples uploaded for Ch 2 are completely live! Granted, this is a malware book and you should expect to see live samples, but the standard to sharing real malware is to at the very least archive it in a ZIP or RAR. That being said, the samples for Ch 5 are not only zipped, they are password protected. This uses your standard password used for sharing samples, but if this is your first exposure to malware, you'll never know the password because I couldn't find it mentioned in the book anywhere. Another issue I found was one of the samples from Ch 2 didn't work (Sality.G.exe) the way the book described it. After looking at the book and the sample downloaded from their blog, the files are not MD5 matches (meaning they are not the same file). Come on...that's just poor practice through and through.

6) There are some (what I believe to be) unnecessary topics. Ch 2 and 3 are completely pointless. Ch 2 goes through 30 pages of submitting multiple files to cuckoo...that's it. No real analysis of what's going on with the sample. It's literally "Here's this command to submit this file. Here's the output in Cuckoo". Ch 3 spends 20 pages on analyzing malware from memory dumps. Yes cuckoo can do memory dumps, but I think this is

a more advanced technique. I don't know why the authors decided to focus on this and not other items, such as the many errors you'll run across with installation. The back of the book states you'll use such tools as [list of tools] but most of them are only a two page mention and don't go into any details.

Maybe I had too high of expectations for this book, but after going through it, it's a complete joke. I honestly can't say this enough - do not buy this book. Even with Amazon's great deals on books, I can't suggest this book to anyone unless it's almost free and even then that's only worsening the situation because then the authors think they did a good job. Do yourself a favor, save the money you would spend on this book and use it towards any other malware analysis book (IDA, Practical Malware Analysis, Malware Analyst Cookbook, etc) or even a Python book. After you do that, read the completely, and always will be, free guide online from the cuckoo developers. If for some reason you need more help, just do an online search for other guides.

1 of 1 people found the following review helpful.
Thrilling and enjoyable read on how to assess for malware
By A. Zubarev
Malware is modern nightmare for any government, enterprises and even private users. No wonder a lot of resources are drained to fight it. Luckily, for budget minded there are Open Source offerings. One of the standing out of the crowd is Cuckoo, written by a Google intern in Python, it constitutes a complete platform for an efficient fight against malware and has an array of enhanced features to offer as impact analysis, reporting to monitoring authorities and issue remediation.

This Packtbook is probably the only offering currently on the market that covers all the intricacies from installing and configuring Cuckoo to extending its capabilities and improving its efficiency further.

The book does not require any programming knowledge nor any special or advanced IT skills, however the author uses an Ubuntu Linux and Oracle VirtualBox (both are extremely popular lately). The book remarkably dedicates alot of time though setting the whole system up, and this is for a reason - malware analysis requires a special approach, persistence and dedication.

The book covers analysis of various malware types and how to attest each, plus involves secondary open source tools, so be prepared to have plenty of hard drive space and enough CPU power.

Despite I did not follow all of the examples it seems that a person on a project would be more than capable to aquatint results with the product in a few days, so if your organization is starting to embrace on a major malware analysis project than look no further than getting this book.I need to state some images appear too small to be read (as most of the report pages) even on a large screen monitor in a PDF.

Some day I am sure will revisit this excellent book and dedicate more time to experimenting with this remarkable, unique software, I was full of excitement and had lots of fun reading this book, hope you will, too.

I am giving this book a 5 out of 5 rating, but I must admit the book is targeting newcomers to the malware fight front using Cuckoo.

1 of 1 people found the following review helpful.
My Review of Cuckoo Malware Analysis
By kellep charles
I had the opportunity to review and conduct some interesting hands-on examples from Packt Publishing’s “Cuckoo Malware Analysis” by Digit Oktavianto and Iqbal Muhardianto. This book was divided into five

intuitive chapters consisting of:

Preface
Chapter 1: Getting Started with Automated Malware Analysis
using Cuckoo Sandbox
Chapter 2: Using Cuckoo Sandbox to Analyze a Sample Malware
Chapter 3: Analyzing the Output of Cuckoo Sandbox
Chapter 4: Reporting with Cuckoo Sandbox
Chapter 5: Tips and Tricks for Cuckoo Sandbox
Index

In chapter one, titled “Getting Started with Automated Malware Analysis
using Cuckoo Sandbox” provided information pertaining to malware analysis methodologies, basic theory in Sandboxing and detailed information on installing the Cuckoo Sandbox framework. The process was not easy, but if directions are followed precisely, then outcome should be favorable. In chapter two “Using Cuckoo Sandbox to Analyze a Sample Malware”, the authors discussed the process of starting Cuckoo as well as submitting various malware samples such as MS Word, MS Excel and PDF documents. In addition, examples to submitting malicious URL, binary files and conducting memory forensics were also demonstrated.

Chapter three “Analyzing the Output of Cuckoo Sandbox” and Chapter four “Reporting with Cuckoo Sandbox”, covered using the processing module and analyzing an APT attack. In addition, the process to creating a built-in reports and exporting data report analysis from Cuckoo to another format were covered.

The last chapter, “Tips and Tricks for Cuckoo Sandbox” pertained informative information about hardening Cuckoo Sandbox against VM detection and other interesting tips I was not to concerned about as a novice in the craft of malware analysis.

Overall, I thought the book was well written as a hybrid tool to learning the process of conducting malware analysis. Chapter one, provided the necessary foundation about malware analysis, while the remaining chapter provided detailed instructions to installing, conducting and reporting malware analysis.

I found this text to be very useful and beneficial for anyone task in conducting the process of malware analysis. In addition, I this text would also provide valuable value in academia as a supplemental text or lab manual.

See all 5 customer reviews...

CUCKOO MALWARE ANALYSIS BY DIGIT OKTAVIANTO, IQBAL MUHARDIANTO PDF

Why should be this on the internet publication **Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto** You might not should go somewhere to check out guides. You could read this book Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto every single time and every where you really want. Also it remains in our extra time or sensation tired of the tasks in the office, this corrects for you. Get this Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto right now and also be the quickest person that finishes reading this book Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto

About the Author

Digit 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.

While the other people in the shop, they are uncertain to discover this Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto straight. It could need more times to go establishment by store. This is why we expect you this site. We will certainly provide the most effective means and also reference to obtain the book Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto Even this is soft data book, it will

be convenience to bring Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto any place or save in the house. The difference is that you might not require move the book Cuckoo Malware Analysis By Digit Oktavianto, Iqbal Muhardianto place to area. You may need only duplicate to the various other gadgets.