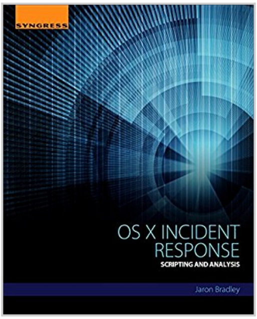

OS X Incident Response: Scripting and Analysis

By Jaron Bradley

OS X Incident Response: Scripting and Analysis By Jaron Bradley

OS X Incident Response: Scripting and Analysis is written for analysts who are looking to expand their understanding of a lesser-known operating system. By mastering the forensic artifacts of OS X, analysts will set themselves apart by acquiring an up-and-coming skillset.

Digital forensics is a critical art and science. While forensics is commonly thought of as a function of a legal investigation, the same tactics and techniques used for those investigations are also important in a response to an incident. Digital evidence is not only critical in the course of investigating many crimes but businesses are recognizing the importance of having skilled forensic investigators on staff in the case of policy violations.

Perhaps more importantly, though, businesses are seeing enormous impact from malware outbreaks as well as data breaches. The skills of a forensic investigator are critical to determine the source of the attack as well as the impact. While there is a lot of focus on Windows because it is the predominant desktop operating system, there are currently very few resources available for forensic investigators on how to investigate attacks, gather evidence and respond to incidents involving OS X. The number of Macs on enterprise networks is rapidly increasing, especially with the growing prevalence of BYOD, including iPads and iPhones.

Author Jaron Bradley covers a wide variety of topics, including both the collection and analysis of the forensic pieces found on the OS. Instead of using expensive commercial tools that clone the hard drive, you will learn how to write your own Python and bash-based response scripts. These scripts and methodologies can be used to collect and analyze volatile data immediately.

For online source codes, please visit:

https://github.com/jbradley89/osx_incident_response_scripting_and_analysis

- Focuses exclusively on OS X attacks, incident response, and forensics
- Provides the technical details of OS X so you can find artifacts that might be

missed using automated tools

- Describes how to write your own Python and bash-based response scripts, which can be used to collect and analyze volatile data immediately
- Covers OS X incident response in complete technical detail, including file system, system startup and scheduling, password dumping, memory, volatile data, logs, browser history, and exfiltration

OS X Incident Response: Scripting and Analysis

By Jaron Bradley

OS X Incident Response: Scripting and Analysis By Jaron Bradley

OS X Incident Response: Scripting and Analysis is written for analysts who are looking to expand their understanding of a lesser-known operating system. By mastering the forensic artifacts of OS X, analysts will set themselves apart by acquiring an up-and-coming skillset.

Digital forensics is a critical art and science. While forensics is commonly thought of as a function of a legal investigation, the same tactics and techniques used for those investigations are also important in a response to an incident. Digital evidence is not only critical in the course of investigating many crimes but businesses are recognizing the importance of having skilled forensic investigators on staff in the case of policy violations.

Perhaps more importantly, though, businesses are seeing enormous impact from malware outbreaks as well as data breaches. The skills of a forensic investigator are critical to determine the source of the attack as well as the impact. While there is a lot of focus on Windows because it is the predominant desktop operating system, there are currently very few resources available for forensic investigators on how to investigate attacks, gather evidence and respond to incidents involving OS X. The number of Macs on enterprise networks is rapidly increasing, especially with the growing prevalence of BYOD, including iPads and iPhones.

Author Jaron Bradley covers a wide variety of topics, including both the collection and analysis of the forensic pieces found on the OS. Instead of using expensive commercial tools that clone the hard drive, you will learn how to write your own Python and bash-based response scripts. These scripts and methodologies can be used to collect and analyze volatile data immediately.

For online source codes, please visit:

https://github.com/jbradley89/osx_incident_response_scripting_and_analysis

- Focuses exclusively on OS X attacks, incident response, and forensics
- Provides the technical details of OS X so you can find artifacts that might be missed using automated tools
- Describes how to write your own Python and bash-based response scripts, which can be used to collect and analyze volatile data immediately
- Covers OS X incident response in complete technical detail, including file system, system startup and scheduling, password dumping, memory, volatile data, logs, browser history, and exfiltration

OS X Incident Response: Scripting and Analysis By Jaron Bradley Bibliography

- Rank: #479314 in Books
- Brand: Bradley Jaron
- Published on: 2016-05-20
- Original language: English

- Number of items: 1
- Dimensions: 9.25" h x .58" w x 7.52" l, .0 pounds
- Binding: Paperback
- 270 pages

Download OS X Incident Response: Scripting and Analysis ...pdf

Read Online OS X Incident Response: Scripting and Analysis ...pdf

Editorial Review

About the Author
Jaron Bradley has a background in host-based incident response and forensics. He entered the information security field as an incident responder immediately after graduating from Eastern Michigan University, where he received his degree in Information Assurance. He now works as a Senior Intrusion Analyst, with a focus on OS X and Linux based attacks.

Users Review

From reader reviews:

Patricia Diaz:

Have you spare time for a day? What do you do when you have much more or little spare time? Yep, you can choose the suitable activity regarding spend your time. Any person spent all their spare time to take a walk, shopping, or went to typically the Mall. How about open or even read a book entitled OS X Incident Response: Scripting and Analysis? Maybe it is being best activity for you. You already know beside you can spend your time using your favorite's book, you can wiser than before. Do you agree with it is opinion or you have different opinion?

Loren Parker:

This OS X Incident Response: Scripting and Analysis is great reserve for you because the content and that is full of information for you who have always deal with world and possess to make decision every minute. This specific book reveal it information accurately using great coordinate word or we can say no rambling sentences within it. So if you are read that hurriedly you can have whole facts in it. Doesn't mean it only will give you straight forward sentences but hard core information with attractive delivering sentences. Having OS X Incident Response: Scripting and Analysis in your hand like obtaining the world in your arm, details in it is not ridiculous one. We can say that no guide that offer you world with ten or fifteen small right but this publication already do that. So , this is good reading book. Hey there Mr. and Mrs. active do you still doubt this?

Bess Cook:

Within this era which is the greater man or woman or who has ability in doing something more are more valuable than other. Do you want to become among it? It is just simple method to have that. What you should do is just spending your time very little but quite enough to possess a look at some books. One of many books in the top collection in your reading list is usually OS X Incident Response: Scripting and Analysis. This book which can be qualified as The Hungry Slopes can get you closer in turning into precious person. By looking way up and review this reserve you can get many advantages.

Brett Nash:

As a scholar exactly feel bored to be able to reading. If their teacher requested them to go to the library as well as to make summary for some guide, they are complained. Just minor students that has reading's spirit or real their pastime. They just do what the teacher want, like asked to go to the library. They go to there but nothing reading really. Any students feel that reading is not important, boring and also can't see colorful photographs on there. Yeah, it is to get complicated. Book is very important for you. As we know that on this era, many ways to get whatever we want. Likewise word says, ways to reach Chinese's country. Therefore , this OS X Incident Response: Scripting and Analysis can make you experience more interested to read.

Download and Read Online OS X Incident Response: Scripting and Analysis By Jaron Bradley #GKPUN7QIFAZ

Read OS X Incident Response: Scripting and Analysis By Jaron Bradley for online ebook

OS X Incident Response: Scripting and Analysis By Jaron Bradley Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read OS X Incident Response: Scripting and Analysis By Jaron Bradley books to read online.

Online OS X Incident Response: Scripting and Analysis By Jaron Bradley ebook PDF download

OS X Incident Response: Scripting and Analysis By Jaron Bradley Doc

OS X Incident Response: Scripting and Analysis By Jaron Bradley Mobipocket

OS X Incident Response: Scripting and Analysis By Jaron Bradley EPub

GKPUN7QIFAZ: OS X Incident Response: Scripting and Analysis By Jaron Bradley