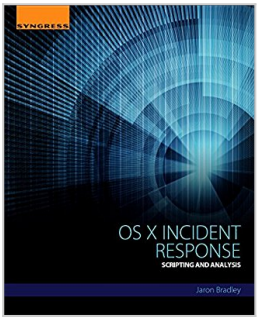

OS X Incident Response: Scripting and Analysis

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

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:

Dolores Watkins:

Why don't make it to be your habit? Right now, try to ready your time to do the important act, like looking for your favorite guide and reading a publication. Beside you can solve your long lasting problem; you can add your knowledge by the e-book entitled OS X Incident Response: Scripting and Analysis. Try to face the book OS X Incident Response: Scripting and Analysis as your close friend. It means that it can to become your friend when you truly feel alone and beside that of course make you smarter than previously. Yeah, it is very fortuned in your case. The book makes you much more confidence because you can know anything by the book. So , we need to make new experience as well as knowledge with this book.

Joyce Cannon:

Now a day those who Living in the era just where everything reachable by connect to the internet and the resources included can be true or not involve people to be aware of each information they get. How individuals to be smart in receiving any information nowadays? Of course the correct answer is reading a book. Studying a book can help persons out of this uncertainty Information specifically this OS X Incident Response: Scripting and Analysis book because book offers you rich facts and knowledge. Of course the information in this book hundred per-cent guarantees there is no doubt in it everbody knows.

Rodolfo Buker:

Are you kind of occupied person, only have 10 or perhaps 15 minute in your day to upgrading your mind talent or thinking skill possibly analytical thinking? Then you are having problem with the book as compared to can satisfy your limited time to read it because this all time you only find e-book that need more time to be read. OS X Incident Response: Scripting and Analysis can be your answer as it can be read by an individual who have those short extra time problems.

Keith Reese:

Beside that OS X Incident Response: Scripting and Analysis in your phone, it can give you a way to get

nearer to the new knowledge or data. The information and the knowledge you may got here is fresh in the oven so don't become worry if you feel like an previous people live in narrow small town. It is good thing to have OS X Incident Response: Scripting and Analysis because this book offers for your requirements readable information. Do you oftentimes have book but you would not get what it's exactly about. Oh come on, that will not happen if you have this inside your hand. The Enjoyable agreement here cannot be questionable, just like treasuring beautiful island. Use you still want to miss it? Find this book as well as read it from today!

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

QDIP2T5RO47: OS X Incident Response: Scripting and Analysis By Jaron Bradley