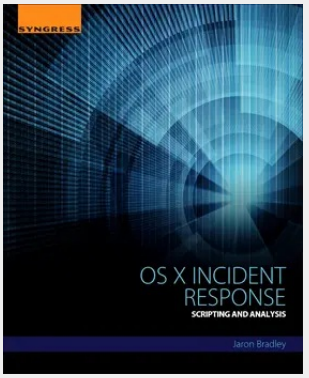
Bradley

OS X Incident Response

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



54,50 €
50,93 € (zzgl. MwSt.)

Nicht mehr lieferbar

Artikelnummer: 9780128044568
Medium: Buch
ISBN: 978-0-12-804456-8
Verlag: Elsevier Science & Technology
Erscheinungstermin: 10.05.2016
Sprache(n): Englisch
Auflage: Erscheinungsjahr 2016
Produktform: Kartoniert
Gewicht: 578 g
Seiten: 270
Format (B x H): 189 x 233 mm