1. Record Nr. UNINA9910254755903321

Autore	Edge Charles S., Jr.
Titolo	Enterprise Mac security : El capitan / / Charles Edge, Daniel O'Donnell
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2016
ISBN	9781484217122 1484217128
Edizione	[Third edition.]
Descrizione fisica	1 online resource (522 p.)
Disciplina	004
Soggetti	Apple computers Computer science Apple and iOS Computer Science, general
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	1. Security Quick-Start -- 2. Services, Daemons, and Processes -- 3. Securing User Accounts -- 4. File System Permissions -- 5. Reviewing Logs and Monitoring -- 6. Application Signing and Sandbox -- 7. Securing Web Browsers and E-mail -- 8. Malware Security: Combating Viruses, Worms, and Root Kits -- 9. Encrypting Files and Volumes -- 10. Securing Network Traffic -- 11. Setting Up the Mac OS X Firewall -- 12. Securing a Wireless Network -- 13.File Services -- 14. Web Site Security -- 15. Remote Connectivity -- 16. Server Security -- 17. Network Scanning, Intrusion Detection, and Intrusion Prevention Tools -- 18. Backup and Fault Tolerance -- 19. Forensics -- 20. Appendix A -- 21. Appendix B -- 22. Appendix C.
Sommario/riassunto	Enterprise Mac Security is a definitive, expert-driven update of the popular, slash-dotted first edition which was written in part as a companion to the SANS Institute course for Mac OS X. It contains detailed Mac OS X security information, and walkthroughs on securing systems, including the new 10.11 operating system. A common misconception in the Mac community is that Mac’s operating system is more secure than others. While this might be have been true in certain cases, security on the Mac has always still been a crucial issue. With the release of OS X 10.11, the operating system is taking large strides in

getting even more secure. Even still, when sharing is enabled or remote control applications are installed, Mac OS X faces a variety of security threats, whether these have been exploited or not. This book caters to both the beginning home user and the seasoned security professional not accustomed to the Mac, establishing best practices for Mac OS X for a wide audience. The authors of this book are seasoned Mac and security professionals, having built many of the largest network infrastructures for Apple and spoken at both DEFCON and Black Hat on OS X security. What You Will Learn The newest security techniques on Mac OS X from the best and brightest Security details of Mac OS X for the desktop and server, and how to secure these systems The details of Mac forensics and Mac hacking How to tackle Apple wireless security Who This Book Is For This book is for new users, switchers, power users, and administrators that need to make sure their Mac systems are secure.