文前

1. 本书配套网站：http://NewOSXBook.com
2. NewOSXBook 论坛：http://NewOSXBook.com/forum/

第 1 章

1．"Pluggable Authentication Modules for Linux" - http://www.linuxjournal.com/article/2120?page= 0,1

2．Apple Open Source - pam_modules project - http://opensource.apple.com/tarballs/pam_modules/

3．Apple Developer - "Open Directory Programming Guide" - https://developer.apple.com/library/mac/documentation/Networking/Conceptual/Open_Directory

4．RFC2307 - "An Approach for Using LDAP as a Network Information Service" - http://www.faqs.org/rffcs/rfc2307.html

5．Apple Developer - Daemons and Services Programming Guide - https://developer.apple.com/library/mac/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingXPCServices.html#//apple_ref/doc/uid/10000172i-SW6-SW1

第 2 章

1．TrustedBSD – “OpenBSM Project” – http://www.trustedbsd.org/openbsm.html

2．Sun Microsystems – “System Administration Guide - Part - VII Solaris Auditing” - http://docs.oracle.com/cd/E19253-01/816-4557/6maosrk4c/index.html

第 3 章

1. “Kernel Authorization” – https://developer.apple.com/library/mac/technotes/tn2127/_index.html

2. Amit Singh – “Mac OS X Internals” Bonus Materials – http://osxbook.com/book/src/

3. “KAuthorama”- https://developer.apple.com/library/mac/samplecode/KauthORama

第 4 章

1．FreeBSD Architecture Handbook, Chapter 6 - https://www.freebsd.org/doc/en_US.ISO8859-1/books/arch-handbook/mac.html

2．FreeBSD Man Pages - Your local FreeBSD man(1) or https://www.freebsd.org/cgi/man.cgi?query=mac_set&sektion=3&apropos=0&manpath=FreeBSD+11-current

第 5 章

1．Apple’s PKI Page – https://www.apple.com/certificateauthority/

2．Apple’s WorldWide Developer Relations Certificate Practice Statement (v1.16) https://www.apple. com/certificateauthority/pdf/Apple_WWDR_CPS_v1.16.pdf

3．Ivan Krstić – “Behind the Scenes with iOS Security” - https://www.blackhat.com/docs/us-16/materials/us-16-Krstic.pdf

4．Tielei, Wang – “Jekyll Apps - When benign apps turn evil”- Usenix Security ’13 https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/wang_tielei

5．Luca Tedesco - iOS 9.2.1 Code Signing Bypass – https://github.com/kpwn/921csbypass

6．Luca Tedesco - iOS 9.3.5 Code Signing Bypass – https://github.com/kpwn/935csbypass

第 6 章

1．DssW - "Authorisation Rights" - https://www.dssw.co.uk/reference/authorization-rights

2．Apple - "OS X: About Gatekeeper" - https://support.apple.com/en-us/HT202491

3．Patrick Wardle - "Exposing Gatekeeper" - https://reverse.put.as/wp-content/uploads/2015/11/Wardle-VB2015.pdf

4．yara - https://github.com/VirusTotal/yara

5．Apple Developer - "Configuration Profile Reference" - https://developer.apple.com/library/prerelease/content/featuredarticles/iPhoneConfigurationProfileRef/

6．Apple Developer - "MDM Protocol Reference" - https://developer.apple.com/library/prerelease/content/documentation/Miscellaneous/Reference/MobileDeviceManagementProtocolRef

7．Marczak & Neagle - "Enterprise Mac Managed Preferences", APress - https://www.amazon.com/gp/product/1430229373/

第 7 章

1．Apple Developer - "iOS App Distribution Guide" - https://developer.appIe.com/library/ios/

documentation/IDEs/Conceptual/AppDistributionGuide/MaintainingProfiles/MaintainingProfiles. html

2. chockenberry GitHub - Provisioning – http://github.com/chockenberry/ProvisioningCydia Impactor - http://cydiaimpactor.com
3. Cydia Impactor - http://cydiaimpactor.com

外部链接

1. P151， https://ppq.apple.com/vl/authorization。

第 8 章

1. Dionysus Balazakis - "The Apple Sandbox" - http://www.semantiscope.com/research/BHDC2011/BHDC2011-Paper.pdf
2. Meder Kydyraliev - "Mining Mach Services within macOS sandbox" - http://2013.zeronights.org/includes/docs/Meder_Kydyraliev_-Mining_Mach_Services_within_OS_X_Sandbox.pdf
3. BSD Manual pages - jail(2) - https://www.freebsd.org/cgi/man.cgi?query=jail&sektion=8#end
4. Stefan Esser - "Sandbox toolkit" - https://github.com/sektioneins/sandbox_toolkit
5. fG! - "Apple's Sandbox Guide- v1.0” - http://reverse.put.as/wp-content/upIoads/2011/09/Apple- Sandbox-Guide-v1.0.pdf

第 9 章

1. Apple - HT204899 - "About System Integrity Protection on your Mac" – https://support.apple.com/en-gb/HT204899
2. Apple- "System Integrity Protection Guide - https://developer.apple.com/library/content/documentation/Security/Conceptual/System_Integrity_Protection_Guide
3. NewOSXBook Forum - "iOS Loading kext" discussion – http://NewOSXBook.com/forum/viewtopic.php?f=7&t=16578#p17140
4. J's Entitlement Database - Companion site forum - http://NewOSXBook.com/ent.jl

第 10 章

1. Apple Discussions Forum - "What the **** is TCCD?" – https://discussions.apple.com/thread/4165543?start=0&tstart=0

2. Apple WWDC 2016 - how iOS Security Really Works – http://devstreaming.apple.com/videos/wwdc/2016/705 s57mrvm8so193i8c/705/705_how_ios_security_really_works.pdf

3. Business Insider - 10/2010 http://www.businessinsider.com/eric-schmidt-we-know-where-you-are-we-know-where-youve-been-we-can-more-or-less-know-what-youre-thinking-about-2010-10

4. Apple, WWDC 2016 "Engineering Privacy For Your Users" - https://developer.apple.com/videos/play/wwdc2016/709

第 11 章

1. Chodary, Gröbert and Metz - "Infiltrate the Vault - Security Analysis and Decryption of Filevault 2", in Advances in Digital Forensics Ⅸ, IFIP Advances in Information and Communication Technology 410, 2013, pp 349-363. – http://eprint.iacr.org/2012/374.pdf

2. fvpres - Chodary, Gröbert and Metz - "Infiltrate the Vault" - Presentation - http://www.cl.cam.ac.uk/~osc22/docs/slides_fv2_ifip_2013.pdf

3. Chodary, Gröbert and Metz - libfvde - https://github.com/libyal/libfvde/

4. Sogeti ESEC, "iPhone data protection in depth" - HITB AMS 2011 - http://esec-lab.sogeti.com/static/publications/11-hitbamsterdam-iphonedataprotection.pdf

5. Sogeti, "iPhone data protection tools" - https://code.google.com/archive/p/iphone-dataprotection/source/default/source

6. Apple - "iOS Security Guide" - https://.www.apple.com/business/docs/iOS_Security_Guide.pdf

7. Ivan Krstić - "Behind the Scenes with iOS Security" - https://www.blackhat.com/docs/us-16/materials/us-16-Krstic.pdf

8. "An Evening With Mobile Obliterator" – http://newosxbook.com/articles/EveningWithMobileObliterator.html

9. Apple Developer - Keychain concepts - https://developer.apple.com/library/content/documentation/Security/Conceptual/keychainServConcepts

10. Mandt, Solnik and Wang - "Demystifying the Secure Enclave Processor" - BH 2016 - https://www.blackhat.com/docs/us-16/materials/us-16-Mandt-Demystifying-The-Secure-Enclave-Processor.pdf

11. FireEye - "Masque Attack: All Your iOS Apps Belong to Us" - https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html

第 12 章

1. Apple - "About OS X NTP Security Update" (TechNote 204425) - https://support.apple.com/ en-us/HT204425
2. Google Project Zero (Röttger and Lord) - Finding and exploiting ntpd vulnerabilities - https://googleprojectzero.blogspot.com/2015/01/finding-and-exploiting-ntpd.html
3. Google Project Zero (Ian Beer) - Issue #343 - https://bugs.chromium.org/p/project-zero/issues/detail?id=343
4. SektionEins - "OS X 10.10 DYLD_PRINT_TO_FILE Local Privilege Escalation Vulnerability" - https://www.sektioneins.de/en/blog/15-07-07-dyld_print_to_file_lpe.html
5. Luis Miras GitHub - https://github.com/luismiras/muymacho
6. Luis Miras - "muymacho, exploiting DYLD_ROOT_PATH" - https://luismiras.github.io/muymacho- exploiting_DYLD_ROOT_PATH/
7. Luca Todesco - "Attacking the XNU Kernel in El Capitan" - https://www.blackhat.com/docs/ eu-15/materials/eu-15-Todesco-Attacking-The-XNU-Kernel-In-El-Capitain.pdf
8. Apple - "About the security content of OS X El Capitan 10.11.1, Security Update 2015-004, etc" - https://support.apple.com/en-us/HT205375
9. OSXReverser - Mach Race - Presentation Slides - https://reverse.put.as/2016/04/27/syscan360-singapore-2016-slides-and-exploit-code/
10. OSXReverser - Mach Race on GitHub - https://github.com/gdbinit/mach_race
11. Ian Beer - "Race you to the Kernel" - https://googleprojectzero.blogspot.sg/2016/03/race-you-to-kernel.html
12. Apple - "Security Content of OS X 10.11.4 and Security Update 2016-002" - https://support.apple.com/en-us/HT206167
13. TrendMicro - "$hell on Earth" - http://documents.trendmicro.com/assets/pdf/shell-on-earth.pdf"
14. KEEN Team - "Subverting Apple Graphics" - http://www.slideshare.net/LiangChen13/us-16subverting-applegraphicspracticalapproachestoremotelygainingrootchenhegrassifu
15. jndok - "Analysis and Exploitation of Pegasus Kernel Vulnerabilities" - http://jndok.github.io/2016/10/04/pegasus-writeup/
16. Brandon Azad - CVE-2016-1828 - https://bazad.github.io/2016/05/mac-os-x-use-after-free/

第 13 章

1．Digital Millennium Copyright Act – http://copyright.gov/fedreg/2015/80fr65944.pdf

2．Apple- HT201954 - "Unauthorized modification of iOS..." - http://support.apple.com/en-us/HT201954

3. PlanetBeing - iOS (32-bit) PatchFinder - https://github.com/planetbeing/ios-jailbreak-patchfinder

4．Luca Tedesco - Yalu (8.4.1 Jailbreak) - https://github.com/kpwn/yalu/blob/master/data/untether/untether64.mm

5. Xerub - "Tick (FPU) Tock (IRQ)" - https://xerub.github.io/ios/kpp/2017/04/13/ticktock.html

6．RFC7693 - "The BLAKE2 Cryptographic Hash and MAC" - http://www.faqs.org/rfcs/rfc7693.html

第 14 章

1. Optiv - Evasi0n Jailbreak's Userland Component - https://www.optiv.com/blog/evasi0n-jailbreaks-userland-component

2．Dowd/Mandt - "From USR to SVC" Azimuth Security – http://blog.azimuthsecurity.com/2013/02/from-usr-to-svc-dissecting-evasi0n.html

3．Mandt - "Attacking the iOS Kernel - A Look at 'evasi0n'" – http://www.nislab.no/content/download/38610/481190/file/NISlecture201303.pdf

4．Evad3rs - Swiping through modern security features – https://conference.hitb.org/hitbsecconf2013ams/materials/”>

5．Companion Web Site – Evasi0n Resources – http://NewOSXBook.com/Resources/ VolIII/Evasi0n/

6．The iPhone Wiki - Firmware Keys – https://www.theiphonewiki.com/wiki/Firmware/iPod_touch#iPod_ touch_4G

7．Dowd/Mandt - "iOS 6 Security" - "http://conference.hitb.org/hitbsecconf2012kul/materials/D1T2%20-%20Mark%20Dowd%20&%20Tarjei%20Mandt%20-%20iOS6%20Security.pdf

8．Dowd/Mandt - "iOS 6 Security" (Video)- https://www.youtube.com/watch?v=O-WZinEoki4

第 15 章

1．Companion Website – Evasi0n 7 files – http://NewOSXBook.com/resources/ev7

2．geoh0t (@tomcr00se) presents an evasi0n7 writeup – http://geohot.com/e7writeup.html

3．Evasi0n 7 - Writeup by P0sixNinja – https://www.theiphonewiki.com/wiki/Evasi0n7#Writeup_by_p0sixninja

4．Breakout - a completely free, open source iOS 7 jailbreak - https://github.com/tihmstar/Breakout

5．WinOCM Blag - "Evading iOS Security" - http://winocm.com/projects/research/2014/01/11/evading_ios_security/index.html

6．Apple - "About the Security Content of iOS 7.1" - https://support.apple.com/en- us/HT202935

外部链接

1． P311，http://evasi0n.com/apple-ipa-info.plist

第 16 章

1．Azimuth Security - "Attacking the iOS 7 PRNG" - Blog post - http://blog.azimuthsecurity.com/2014/03/attacking-ios-7-earlyrandom-prng.html

2．Azimuth Security - "Attacking the iOS 7 PRNG" - White Paper - http://mista.nu/research/early_random-paper.pdf

3．Apple - "About the security content of iOS 8" - https://support.apple.com/en-us/HT201395

外部链接

1． P328，pangu.io

2． P328，en.7.pangu.io

第 17 章

1．@PanguTeam - "The Userland Exploits of Pangu 8" - https://cansecwest.com/slides/2015/CanSecWest2015_Final.pdf

2．Apple - "About the security content of iOS 8.1.1" - https://suppor.apple.com/en-us/HT204418

第 18 章

1．The annotated informal guide to TaiG - Ⅰ – http://newosxbook.com/articles/TaiG.html

2．The annotated informal guide to TaiG - Ⅱ – http://newosxbook.com/articles/TaiG2.html

3．Proteas of Qihoo 360 Team Nirvan - “iOS 8.1.2 越狱过程详解及相关漏洞分析”(iOS 8.1.2 jailbreak process detailed and related vulnerability analysis) - http://nirvan.360.cn/blog/?p=887

4．SektionEins - "mach_port_kobject() and the kernel address obfuscation" - https://www.sektioneins.de/en/blog/14-12-23-mach_port_kobject.html

5．Apple - "About the security content of iOS 8.1.3" - https://support.apple.com/en-us/HT204245

第 19 章

1．"Open Source TaiG", https://github.com/stefanesser/opensource_taig

2．"TaiG 2 (Part the 1st)", http://NewOSXBook.com/articles/28Dayslater.html

3．"TaiG 2 (Part the 2nd)", http://NewOSXBook.com/articles/HIDeAndSeek.html

4．Pangu Team Blog - "CVE-2015-5774" - http://blog.pangu.io/cve-2015-5774/

5．360 Nirvan Team - "CVE-2015-5774 分析及利用(Analysis & exploitation)" - http://nirvan.360.cn/blog/?p=461

第 20 章

1．"Hacking from iOS 8 to iOS 9" - Team Pangu - http://blog.pangu.io/wp-content/uploads/2015/11/ POC2015_RUXCON2015.pdf

2．"Pangu 9 Internals" - Team Pangu - https://www.blackhat.com/docs/us-16/materials/us-16-Wang-Pangu-9-Internals.pdf

第 22 章

1. Citizen Lab - "The Million Dollar Dissident" -
https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
2. Max Bazaliy, LookOut security - "Technical Analysis of the Pegasus Exploits on iOS" -
https://info.lookout.com/rs/051-ESQ-475/images/pegasus-exploits-technical-details.pdf"
3. Max Bazaliy, Blackhat Europe 2016 - https://speakerdeck.com/mbazaliy/mobile-espionage-in-
the-wild-pegasus-and-nation-state-level-attacks
4. Max Bazaliy, CCC 2016 - https://www.youtube.com/watch?v=riRcYwOvamY
5. Stefan Esser - sektioneins.de/en/blog/16-09-02-pegasus-ios-kernel-vulnerability-explained.html
6. Min ("Spark") Zheng - Local Privilege Escalation for OS X via PEGASUS -
https://github.com/zhengmin1989/OS-X-10.11.6-Exp-via-PEGASUS
7. jndok - "Analysis and Exploitation of Pegasus Kernel Vulnerabilities" -
http://jndok.github.io/2016/10/04/pegasus-writeup/
8. AngelXWind - GitHub - http://github.com/angelXwind/Trident

第 22.5 章

1. Ian Beer (Project Zero) - "Multiple Memory Safety Issues in mach_ports_register" -
https://bugs.chromium.org/p/project-zero/issues/detail?id=882

第 23 章

1. Ben Hawkes - Twitter - https://twitter.com/benhawkes/status/808439576238792704
2. Ian Beer - "XNU kernel UaF due to lack of locking in set_dp_control_port" -
3. Project Zero Blog - https://bugs.chromium.org/p/project-zero/issues/detail?id=965#c2
4. Apple - "Security Content of iOS 10.2" - https://support.apple.com/en-us/HT207422

第 24 章

1. Ian Beer - 10.2 Jailbreak PoC -
https://bugs.chromium.org/p/project-zero/issues/attachment?aid=268352
2. Yalu102 - GitHub - https://github.com/kpwn/yalu102/
3. Ian Beer (Project Zero) - "iOS/MacOS kernel memory corruption.."
https://bugs.chromium.org/p/project-zero/issues/detail?id=1004
4. LiberTV - NewOSXBook.com forum - http://newosxbook.com/forum