# The Hacker's Guide to OS X

## Exploiting OS X from the Root Up

Rob Bathurst

Russ Rogers

Alijohn Ghassemlouei

Pat Engebretson,Technical Editor

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an Imprint of Elsevier

SYNGRESS

# Contents

FOREWORD ........ ix

**CHAPTER 1** Introduction ........ 1

Why You are Reading This Book? ........ 1

What is Contained Within the Guide? ........ 2

The Path Ahead ........ 4

References ........ 4

**CHAPTER 2** History and Introduction to OSX ........ 5

History and Introduction to OSX ........ 5

OSX Origins ........ 5

Common Misconceptions ........ 9

Perceptions ........ 11

Capabilities ........ 11

Environments Leveraging OSX ........ 12

What Next? ........ 16

**CHAPTER 3** The Filesystem ........ 17

Introduction ........ 17

What is a File System? ........ 17

The Difference Between Memory Types ........ 18

Partition Tables ........ 19

Booting ........ 22

Working up to HFS+ ........ 24

How a File System Works ........ 25

Disk Fragmentation ........ 27

The File System Forefathers ........ 28

HFS Plus ........ 34

Journaled HFS ........ 35

MetaData ........ 36

Understanding Forks ........ 38

Fiddling with the File System ........ 41

Playing with Attributes.....41
Hidden Files.....43
Conclusion.....46

CHAPTER 4 Footprinting OSX.....49
Introduction.....49
Off the Client.....50
On the Client.....69
Conclusion.....77

CHAPTER 5 Application and System Vulnerabilities.....79
Introduction.....79
Understanding Vulnerabilities.....79
Vulnerabilities are Equal Opportunity.....83
History of Vulnerabilities in Apple Products.....85
Mac OS X Specific.....86
A Recent Example—Flashback.....88
Apple iOS Specific.....91
Advanced Persistent Threats.....94
Apple Script.....95
Conclusion.....100

CHAPTER 6 Defensive Applications.....101
Introduction.....101
Secure Configurations.....102
Passwords, Passphrases, and Multi-Factor Authentication.....102
Account Access Restriction.....103
FileVault.....106
Firewall Configuration.....108
Network Services.....111
Kernel Extension Removal.....114
Examining Commercial Tools.....117
PrivacyScan by SecureMac.....117
MacScan by SecureMac.....124
Conclusion.....135

CHAPTER 7 Offensive Tactics.....137
Introduction.....137
The Exploits.....139
Using the Ammo in the Weapon.....143
Summary.....156
References.....157

CHAPTER 8 Reverse Engineering ........ 159
Introduction ........ 159
The Basics ........ 160
Coding ........ 161
Decompiling Journey ........ 166
Analysis Techniques ........ 182
References ........ 183

CHAPTER 9 Mobile Platforms ........ 185
Introduction ........ 185
Apple iOS Security Model and Overview ........ 186
Insecurity Overview ........ 189
The Goods ........ 198
Please Don't Hurt My Toys ........ 203
Summary ........ 204
References ........ 205

CHAPTER 10 Mac OS X Tips and Tricks ........ 207
Introduction ........ 207
Web Browser Plugins ........ 207
Offensive Plugins ........ 208
Defensive Plugins ........ 219
Cool OS X hacks ........ 223
Safari Debug Mode ........ 223
Total Mac OS X Inversion ........ 224
More on ACP Applications ........ 225
Conclusion ........ 228

INDEX ........ 229