Rootkits and Invisible Software

creating and revealing

by HackingSchool.com

Title: Rootkits and invisible software. Creating and revealing.

Copyright © by Hacking School – CSH Press.
All Rights Reserved.

All rights reserved. This publication is protected by copyright. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior consent of the publisher.

Company or product names mentioned herein are the trademarks or registered trademarks of their respective owners.

The author and the publisher have taken care to ensure the information in this publication is reliable and complete, but cannot assume responsibility for its use and for any related potential breach of patents or copyright. The author and the publisher cannot assume responsibility for any consequences or damage in connection with the use of the information in this publication.

Feel free to contact us:
contact@hackingschool.com

For the latest information about this publication, go to http://www.HackingSchool.com.

Feel free to check out our other IT security and hacking courses available on

www.HackingSchool.com

Your special coupon code (30% OFF!): RKIT30

Use the coupon code to buy our other courses

Table of contents

Legal information **9**
Note re: antiviruses 15

Module 1. Intro and environment setup **17**
Foreword 17
What is a rootkit? 17
Rootkit structure 18
Examples of rootkits 18
What you need to know to start 18
Compatibility and current code version 19
Further reading 19
Practice: video module transcript 20

Module 2. Basics of shellcode development **33**
Assembly language crash course 33
Register types 33
Instruction syntax 34
Writing shellcode 37
Shellcode writing: the essentials 37
Glossary 38
Code injection 38
Notes about the 64-bit architecture 39
Practice: video module transcript 39

Module 3.1. Hiding processes **47**
Intro 47
Theory 47
Writing rootkit code 49
Hiding processes 55
Practice: video module transcript 63

Module 3.2. Hiding files and directories **75**
Hiding files and directories 75
Practice: video module transcript 81

Module 3.3. Hiding registry entries **91**
Intro 91
Notes about the 64-bit mode 93
Practice: video module transcript 96

Module 4.1. Creating a backdoor, implementation of a keylogger **103**
Creating a backdoor to a system 103
Keylogger 104
Taking a screenshot 113
Sending logs 115
Autorun 117
Practice: video module transcript 118

Module 4.2. Remote console **131**
Remote console 131
Practice: video module transcript 137

Module 5. Windows security features **147**
What defense mechanisms are included in Windows? 147
Practice: video module transcript 149

Module 6.1. Creating undetectable applications **157**
Understanding how antiviruses detect threats 157
Signatures 157
Practice: video module transcript 159

Module 6.2. Deceiving a heuristic scanner **165**
Heuristics 165
Practice: video module transcript 166

Module 6.3. Anti-emulation techniques **171**
Emulation 171
RC4 overview 171
System calls and 64-bit architecture 174
Practice: video module transcript 176

Module 7. Bypassing the firewall **183**
Modifying the remote console 190
Practice: video module transcript 191

Module 8. Keeping a rootkit in a system **199**
Areas for hiding programs 199
Running a program as a system service 204
Dll spoofing 205
Practice: video module transcript 207

Module 9. Defense **219**
Rootkit detectors 219
Practice: video module transcript 227

Module 10. Rootkit development and summary **239**
Rootkit development and summary 249
Wrapping up