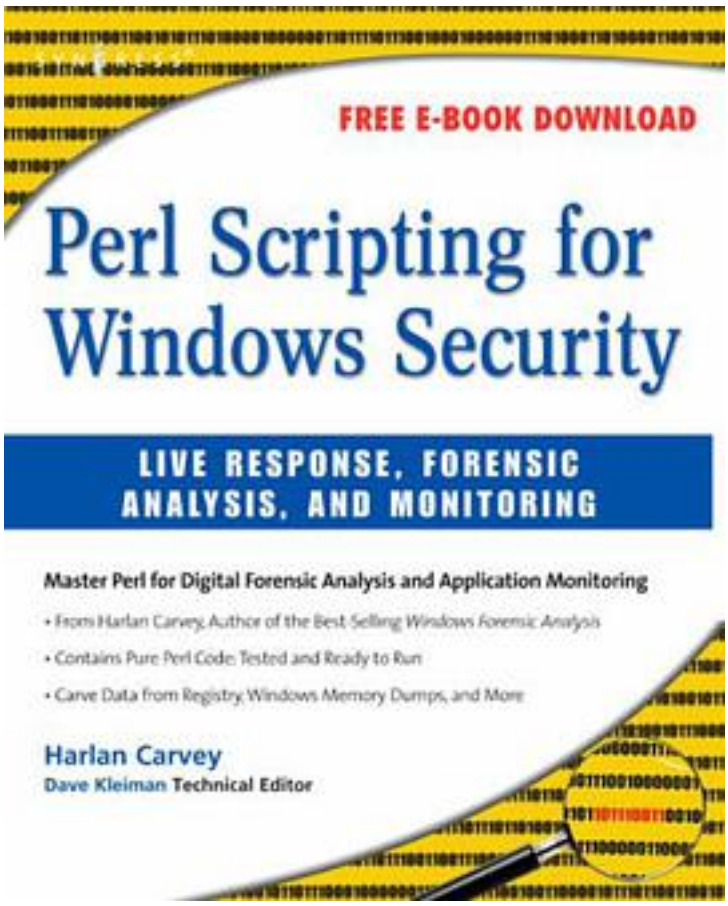
Perl Scripting for Windows Security



Perl Scripting for Windows Security_下载链接1_

著者:Harlan Carvey

出版者:Elsevier Inc.

出版时间:2007-12-26

装帧:Paperback

isbn:9781597491730

I decided to write this book for a couple of reasons. One was that I've now written a couple of books that have to do with incident response and forensic analysis on Windows systems, and I used a lot of Perl in both books. Okay. I'll come clean. I used nothing but Perl in both books! What I've seen as a result of this is that many readers

want to use the tools, but don't know how they simply aren't familiar with Perl, with interpreted (or scripting) languages in general, and may not be entirely comfortable with running tools at the command line. This book is intended for anyone who has an interest in useful Perl scripting, in particular on the Windows platform, for the purpose of incident response, and forensic analysis, and application monitoring. While a thorough grounding in scripting languages (or in Perl specifically) is not required, it helpful in fully and more completely understanding the material and code presented in this book. This book contains information that is useful to consultants who perform incident response and computer forensics, specifically as those activities pertain to MS Windows systems (Windows 2000, XP, 2003, and some Vista). My hope is that not only will consultants (such as myself) find this material valuable, but so will system administrators, law enforcement officers, and students in undergraduate and graduate programs focusing on computer forensics. Code can be found at our associated website. Perl Scripting for Live Response - using Perl, there's a great deal of information you can retrieve from systems, locally or remotely, as part of troubleshooting or investigating an issue. Perl scripts can be run from a central management point, reaching out to remote systems in order to collect information, or they can be 'compiled' into standalone executables using PAR, PerlApp, or Perl2Exe so that they can be run on systems that do not have ActiveState's Perl distribution (or any other Perl distribution) installed. Perl Scripting for Computer Forensic Analysis - Perl is an extremely useful and powerful tool for performing computer forensic analysis. While there are applications available that let an examiner access acquired images and perform some modicum of visualization, there are relatively few tools that meet the specific needs of a specific examiner working on a specific case. This is where the use of Perl really shines through and becomes apparent. Perl Scripting for Application Monitoring - working with enterprise-level Windows applications requires a great deal of analysis and constant monitoring. Automating the monitoring portion of this effort can save a great deal of time, reduce system downtimes, and improve the reliability of your overall application. By utilizing Perl scripts and integrating them with the application technology, you can easily build a simple monitoring framework that can alert you to current or future application issues.

作者介绍:

目录:

Perl Scripting for Windows Security_下载链接1_

标签

评论

Perl Scripting for Windows Security_下载链接1_

书评

Perl Scripting for Windows Security_下载链接1_