DESCRIPTION

Defend your networks and data from attack with this unique two-book security set

The Attack and Defend Computer Security Set is a two-book set comprised of the bestselling second edition of Web Application Hacker's Handbook and Malware Analyst's Cookbook. This special security bundle combines coverage of the two most crucial tactics used to defend networks, applications, and data from attack while giving security professionals insight into the underlying details of these attacks themselves.

The Web Application Hacker's Handbook takes a broad look at web application security and exposes the steps a hacker can take to attack an application, while providing information on how the application can defend itself. Fully updated for the latest security trends and threats, this guide covers remoting frameworks, HTML5, and cross-domain integration techniques along with clickjacking, framebusting, HTTP parameter pollution, XML external entity injection, hybrid file attacks, and more.

The Malware Analyst's Cookbook includes a book and DVD and is designed to enhance the analytical capabilities of anyone who works with malware. Whether you're tracking a Trojan across networks, performing an in-depth binary analysis, or inspecting a machine for potential infections, the recipes in this book will help you go beyond the basic tools for tackling security challenges to cover how to extend your favorite tools or build your own from scratch using C, Python, and Perl source code. The companion DVD features all the files needed to work through the recipes in the book and to complete reverse-engineering challenges along the way.

The Attack and Defend Computer Security Set gives your organization the security tools needed to sound the alarm and stand your ground against malicious threats lurking online.
SET COMPONENTS

Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code
Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard
$59.99

Dafydd Stuttard, Marcus Pinto
$50.00

ABOUT THE AUTHOR

Dafydd Stuttard has more than 10 years' experience in the area of web application security. He is the lead author of Web Application Hacker's Handbook 1e and 2e, has performed penetration testing training around the world.

Marcus Pinto is co-author of Web Application Hacker's Handbook 1e and 2e and has over 10 years' experience within web application security. He has delivered a variety of training courses to technical audiences and speaks at security events around and outside of the UK.

Michael Hale Ligh is the lead author of The Malware Analyst's Cookbook and Director of Malware Research of the The Volatility Project. Michael is a regular presenter at DefCon conferences.

Matt Richard is and is the Malicious Code Operations Lead at Raytheon Corporation and has written a number of testing tools.
Steven Adair is a security researcher with The Shadowserver Foundation and co-author of The Malware Analyst's Cookbook and deals with cyber attacks of all kinds esp. those linked to cyber espionage.

Blake Hartstein conducts incident response and intrusion detection for Bloomberg and previously for VeriSign. The biggest and best companies worldwide depend on him for intelligence about attacks affecting their organization.
To purchase this product, please visit https://www.wiley.com/en-us/9781118906736