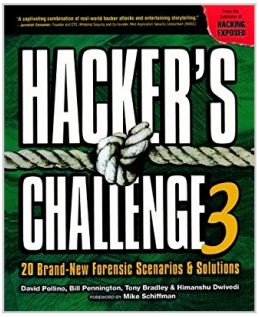

Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3)

By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi

Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi

The stories about phishing attacks against banks are so true-to-life, it's chilling." --Joel Dubin, CISSP, Microsoft MVP in Security

Every day, hackers are devising new ways to break into your network. Do you have what it takes to stop them? Find out in *Hacker's Challenge 3*. Inside, top-tier security experts offer 20 brand-new, real-world network security incidents to test your computer forensics and response skills. All the latest hot-button topics are covered, including phishing and pharming scams, internal corporate hacking, Cisco IOS, wireless, iSCSI storage, VoIP, Windows, Mac OS X, and UNIX/Linux hacks, and much more. Each challenge includes a detailed explanation of the incident--how the break-in was detected, evidence and clues, technical background such as log files and network maps, and a series of questions for you to solve. In Part II, you'll get a detailed analysis of how the experts solved each incident.

Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3)

By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi

Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi

The stories about phishing attacks against banks are so true-to-life, it's chilling." --Joel Dubin, CISSP, Microsoft MVP in Security

Every day, hackers are devising new ways to break into your network. Do you have what it takes to stop them? Find out in *Hacker's Challenge 3*. Inside, top-tier security experts offer 20 brand-new, real-world network security incidents to test your computer forensics and response skills. All the latest hot-button topics are covered, including phishing and pharming scams, internal corporate hacking, Cisco IOS, wireless, iSCSI storage, VoIP, Windows, Mac OS X, and UNIX/Linux hacks, and much more. Each challenge includes a detailed explanation of the incident--how the break-in was detected, evidence and clues, technical background such as log files and network maps, and a series of questions for you to solve. In Part II, you'll get a detailed analysis of how the experts solved each incident.

Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi Bibliography

- Sales Rank: #1076004 in Books
- Published on: 2006-05-16
- Released on: 2006-04-25
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x .84" w x 7.30" l, 1.47 pounds
- Binding: Paperback
- 400 pages

Editorial Review

From the Back Cover

The stories about phishing attacks against banks are so true-to-life, it's chilling." --Joel Dubin, CISSP, Microsoft MVP in Security

Every day, hackers are devising new ways to break into your network. Do you have what it takes to stop them? Find out in *Hacker's Challenge 3*. Inside, top-tier security experts offer 20 brand-new, real-world network security incidents to test your computer forensics and response skills. All the latest hot-button topics are covered, including phishing and pharming scams, internal corporate hacking, Cisco IOS, wireless, iSCSI storage, VoIP, Windows, Mac OS X, and UNIX/Linux hacks, and much more. Each challenge includes a detailed explanation of the incident--how the break-in was detected, evidence and clues, technical background such as log files and network maps, and a series of questions for you to solve. In Part II, you'll get a detailed analysis of how the experts solved each incident.

Exerpt from "Big Bait, Big Phish":

The Challenge: "Could you find out what's going on with the gobi web server? Customer order e-mails aren't being sent out, and the thing's chugging under a big load…" Rob e-mailed the development team reminding them not to send marketing e-mails from the gobi web server…. "Customer service is worried about some issue with tons of disputed false orders…." Rob noticed a suspicious pattern with the "false" orders: they were all being delivered to the same P.O. box…He decided to investigate the access logs. An external JavaScript file being referenced seemed especially strange, so he tested to see if he could access it himself…. The attacker was manipulating the link parameter of the login.pl application. Rob needed to see the server side script that generated the login.pl page to determine the purpose….

The Solution: After reviewing the log files included in the challenge, propose your assessment: What is the significance of the attacker's JavaScript file? What was an early clue that Rob missed that might have alerted him to something being amiss? What are some different ways the attacker could have delivered the payload? Who is this attack ultimately targeted against? Then, turn to the experts' answers to find out what really happened.

About the Author

David Pollino has a strong background in security, wireless, and networking. David is currently a security practitioner working in financial services. During his career, he has worked for an industry-leading security consulting company, a large financial services company, and a tier 1 ISP. David often speaks at security events and has frequently been quoted in online and printed journals regarding security issues. During his career as a consultant and network engineer, David has worked for clients across multiple industries, including financial services, service providers, high technology, manufacturing, and government. He co-authored *Wireless Security* (RSA Press, 2002) and *Hacker's Challenge* and *Hacker's Challenge 2* (McGraw-Hill/Osborne, 2001 and 2002, respectively).

Bill Pennington, CISSP, has six years of professional experience in information security and eleven years in

information technology. His duties at WhiteHat include managing research and development, guiding product and technology direction, managing web application assessment teams, and developing and delivering WhiteHat Security training. Bill has performed web application assessments for more than four years in a variety of industry verticals including financial services, e-commerce, and biotechnology. He is familiar with Mac OS X, Linux, Solaris, Windows, and OpenBSD, and he is a Certified Information Security Systems Practitioner (CISSP) and Certified Cisco Network Administrator (CCNA). He has broad experience in web application security, penetration testing, computer forensics, and intrusion detection systems. Prior to joining WhiteHat, Bill was a principal consultant and technical lead for assessment services at Guardent, a nationwide security services provider.

Tony Bradley, CISSP-ISSAP, MCSE2k, has eight years of computer networking and administration experience, focusing the last four on network security and malware protection. Tony is a network security architect providing design, implementation, and management of network security solutions for a variety of Fortune 500 customers. He is also the editor and writer for the About.com Internet/Network Security website and frequently contributes to a variety of technical and security publications, both in print and on the Web. You can view his writing portfolio at http://www.s3kur3.com.

Himanshu Dwivedi is a founding partner of iSEC Partners, an independent provider of information security services and tools. He has 12 years of experience in security and IT. Before forming iSEC, he was Technical Director for @stake's Bay Area security practice. Himanshu's professional focus includes strategic security services, which leverages his experience with software development, infrastructure security, application security, tool development, and secure product design. He is considered an industry expert in storage security, specifically Fibre Channel/iSCSI SANs and CIFS/NFS NAS systems. Himanshu has presented at major security conferences throughout the world, including Black Hat, Storage Networking World, Syscan Singapore, and Bellua Indonesia. Himanshu also has a patent pending for a storage security design architecture that can be implemented on enterprise storage products for Fibre Channel networks. Himanshu has also authored two additional security books, including *Securing Storage: A Practical Guide to SAN and NAS Security* (Addison-Wesley, 2005) and *Implementing SSH: Strategies for Optimizing the Secure Shell* (Wiley, 2003).

Users Review

From reader reviews:

Lauren Graves:

What do you concentrate on book? It is just for students because they're still students or this for all people in the world, the particular best subject for that? Just simply you can be answered for that question above. Every person has various personality and hobby per other. Don't to be pushed someone or something that they don't would like do that. You must know how great as well as important the book Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3). All type of book can you see on many methods. You can look for the internet methods or other social media.

Randall Hernandez:

Now a day people who Living in the era everywhere everything reachable by talk with the internet and the resources in it can be true or not call for people to be aware of each info they get. How many people to be smart in getting any information nowadays? Of course the answer is reading a book. Examining a book can help folks out of this uncertainty Information particularly this Hacker's Challenge 3: 20 Brand New Forensic

Scenarios & Solutions (Networking & Communication - OMG) (v. 3) book because book offers you rich info and knowledge. Of course the data in this book hundred % guarantees there is no doubt in it you may already know.

Michael Hansen:

Reading a book being new life style in this 12 months; every people loves to go through a book. When you read a book you can get a large amount of benefit. When you read ebooks, you can improve your knowledge, due to the fact book has a lot of information onto it. The information that you will get depend on what types of book that you have read. If you would like get information about your research, you can read education books, but if you want to entertain yourself you can read a fiction books, this sort of us novel, comics, and soon. The Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) offer you a new experience in reading through a book.

Leah Humphries:

In this period globalization it is important to someone to find information. The information will make anyone to understand the condition of the world. The health of the world makes the information simpler to share. You can find a lot of recommendations to get information example: internet, paper, book, and soon. You can view that now, a lot of publisher that print many kinds of book. The particular book that recommended to you is Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) this publication consist a lot of the information in the condition of this world now. This particular book was represented how do the world has grown up. The dialect styles that writer require to explain it is easy to understand. Often the writer made some investigation when he makes this book. That is why this book ideal all of you.

Read Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi for online ebook

Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi books to read online.

Online Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi ebook PDF download

Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi Doc

Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi Mobipocket

Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions (Networking & Communication - OMG) (v. 3) By David Pollino, Bill Pennington, Tony Bradley, Himanshu Dwivedi EPub