IT Security Interviews Exposed: Secrets to Landing Your Next Information Security Job

Chris Butler, Russ Rogers, Mason Ferratt, Greg Miles, Ed Fuller, Chris Hurley, Rob Cameron, Brian Kirouac

*ebooks | Download PDF | *ePub | DOC | audiobook*

#615257 in Books 2007-07-23Original language:EnglishPDF # 1 9.20 x .50 x 7.41l, .75 #File Name: 0471779873244 pages | File size: 71.Mb

Chris Butler, Russ Rogers, Mason Ferratt, Greg Miles, Ed Fuller, Chris Hurley, Rob Cameron, Brian Kirouac : IT Security Interviews Exposed: Secrets to Landing Your Next Information Security Job before purchasing it in order to gage whether or not it would be worth my time, and all praised IT Security Interviews Exposed: Secrets to Landing Your Next Information Security Job:

18 of 19 people found the following review helpful. Good review for a pro, but not meant for a newbie.By Ben RothkeInformation security is a hot career area and is among the strongest fields within IT for growth and opportunity. With excellent long-term career prospects, increasing cybersecurity vulnerabilities and an increase in security privacy regulations and legislation, the demand for security professionals is significant. Even with a bright future, that does not necessarily mean that a career in information security is right for everyone. What differentiates an excellent security

professional from a mediocre one is their passion for the job. With that, IT Security Interviews Exposed is a mixed bag of a book. For those that are looking for an information security spot and have the requisite passion for the job, much of the information should already be known. For someone who lacks that passion and simply wants a security job, their lack of breadth will show and the information in the book likely won't be helpful, unless they have a photographic memory to remember all of the various data points.If you find information security challenging and either want a job in the field or are looking for a better job in the field, the book will be quite valuable. But for those looking for a hot security job, their lackings will likely show through on in interview, even with the help of this book.As to the actual content, chapter 1 provides a good overview of how to find, interview and get a security job. The chapter contains many bits of helpful information, especially to those whose job seeking skills are deficient. A good piece of advice the author's state is that one should never pay a fee for headhunting services. There are many people that call themselves recruiters, but are nothing more than fax servers who charge for the service. The burden to pay is always on the hiring firm, and a job seeker should be extremely suspicious of anyone requesting a fee to find them a position.I would hope that in future editions of the book, the authors expand on chapter one. The chapter itself in fact could easily me made into a book in its own right. As part of the job search process, many job searchers often do not ask themselves enough fundamental questions if they are indeed in the right place in their career. Such an approach is taken by Lee Kushner, founder and CEO of the information security recruitment firm LJ Kushner and Associates. Kushner formulated the following 7 questions that every information security job candidate should ask themselves:1. What are my long and short term plans?2. What are my strengths and weaknesses?3. What skills do I need to develop?4. Have I acquired a new skill during the past year?5. What are my most significant career accomplishments and will I soon achieve another one?6. Have I been promoted over the past three years?7. What investments have I made in my own career?The other 9 chapters of the book all have the same format; an overview of the topic, and then various questions and interviewer may pose. The reality that these topics of network and security fundamentals, firewalls, regulations, wireless, security tools, and more, are essential knowledge for a security professional. Anyone trying to go through a comprehensive information security interview and wing it by reviewing the material will likely only succeed if the interviewer is inept. Anyone attempting to mimic the questions and answers in the book in a real-world interview will immediately be found to be a sham if the interviewer deviates even slightly from the script, which should be expected.What really separates a good candidate from a great candidate is hands-on, practical and real-world security experience. Such a candidate won't need a question and answer format to showcase themselves in an interview. Their experience should shine, and not their ability to rattle of security acronyms.If a company is serious about hiring qualified people, the interview process should not be about short technical questions and acronym definitions. It should entail an open discussion with significant give and take. Having a candidate detail their methodology for deploying and configuring a firewall should be given more credence than their ability to define the TCP the three-way handshake.Ultimately, the efficacy of the book is in the disposition of the reader. For the security newbie who wants a crash course in security in order to quickly land a security job, heaven help the company that would hire such a person. While one should indeed not judge a book by its cover; this book's cover and title may lead some readers to think that the book is their golden ticket to a quick landing into a great career. The breadth of information that a security professional needs to know precludes and short of cramming or quick introductions. Those with a lack of security experience attempting to use this book to hide their shortcomings will only embarrass themselves on an interview.On the other hand, for the reader who has a background in information security who wants an update on network and security fundamentals, they will find IT Security Interviews Exposed a helpful title. The book contains a plethora of valuable information written in a clear and easy to read style. In a little over 200 pages, the book is able to provide the reader with a good review of what they know or may have forgotten. Used in such a setting by such a reader makes the book a most helpful tool for the serious security professional looking to advance their career.1 of 1 people found the following review helpful. Good short guide to prep before an interview.By X. LiuI agree with some of the other reviewers there are some chapters that can be left out of this book. Some topics such as ethics and laws would probably never get asked in an interview. This is slightly biased by my own experience since I lean towards the more technical side.This is a good interview book for a newbie. The network chapter is especially helpful for a quick overview on the fundamentals such as the 7 layer OSI model and the type of attacks and mitigation that can be implemented at each layer.4 of 5 people found the following review helpful. Misleading titleBy Vo BlinnThe book, despite the title, is mostly about networking and relatedsecurity issues.Less than 40 pp (out of ~240) devoted to- ethics,- risk (2 pages),in Ch. 3 and regulations in Ch. 4.Not without some editorial mistakes- ViFi for 802.11x, p. 24: apart from spelling, 802.11x familystandardizes WLAN communication, while WiFi is used in product branding.Some are more dangerous:- Managing these connections using well-defined ports(or sockets when combined with the source IP address) is vital ..., p. 24:well-defined, while not defined, are easily confusable with well-known ports.Which might be a hint on why it has not seen 2nd edition, in spite ofgrowing popularity of the profession.Regrettably there are only few publications on the subject.

Technology professionals seeking higher-paying security jobs need to know security fundamentals to land the job-and

this book will help Divided into two parts: how to get the job and a security crash course to prepare for the job interview Security is one of today's fastest growing IT specialties, and this book will appeal to technology professionals looking to segue to a security-focused position Discusses creating a resume, dealing with headhunters, interviewing, making a data stream flow, classifying security threats, building a lab, building a hacker's toolkit, and documenting work The number of information security jobs is growing at an estimated rate of 14 percent a year, and is expected to reach 2.1 million jobs by 2008

"The book is readable and written in a light, witty style". (Info Security, September 2007)From the Back CoverIt's not a job. It's THE job, and here's how to get it. What does your ideal IT security job look like? What will prospective employers expect you to know? What affects how they view you and your skills? What if you haven't had much experience? What if you're not 30 anymore? Here's the crash course in how to discover, apply for, and land the IT security job you want. Written by a squad of highly credentialed security professionals, this guide prepares you with the technical knowledge, interview skills, strategies, and job search techniques you need to find and get the perfect job. Meet every job search challenge What does and doesn't belong on your rsum How to survive a telephone interview All about firewall technologies, devices, deployment strategies, and management A review of security essentials, regulations, legislation, and guidelines The effects of state cyber security laws, Sarbanes-Oxley, and international standards A refresher course in network fundamentals Everything you should know about wireless, security posture, and tools When and how to say "no" About the AuthorChris Butler (CISSP, JNCIS-FWV, JNCIA-SSL, CCSE, IAM/IEM) is a Senior Solutions Architect with Intellitactics. Chris has more than a dozen years of experience in the networking and security fields. He is a veteran of the United States Navy, where he worked in the cryptography field. Chris has designed, implemented, and supported some of the largest networks in the country for large insurance companies, investment firms, software companies, service providers, and pharmaceutical companies. He has also provided network and security consulting services for numerous U.S. government agencies, including the Department of State, Department of Defense, and the Department of Energy. He has worked extensively with the leading security and networking vendors throughout his career. He is also well versed in both commercial and open source network and security management software. Chris has also performed in-depth application analysis and network modeling using OPNET software for dozens of large companies. He is a member of the IEEE Computer Society and SANS. Russ Rogers (CISSP, IAM/IEM) is a Senior Cyber Security Analyst and the former CEO and co-founder of Security Horizon, Inc. Russ is a United States Air Force veteran and has served in military and contract support for the National Security Agency, Defense Information Systems Agency, and the other federal agencies. He is also the editor-in-chief of The Security Journal. Additionally, he serves as the Professor of Network Security at the University of Advancing Technology (uat.edu) in Tempe, Arizona. Russ is the author, co-author, or technical editor for nearly a dozen books on information security. Russ has spoken and provided training to audiences around the world and is also a co-founder of the Security Tribe information security research Web site at www.securitytribe.com. His education includes a bachelors and masters degree from the University of Maryland in Computer Science areas. Mason Ferratt (JNCIS-FWV, JNCIA-M MSEE, BSME) is a Federal Systems Engineer with Juniper Networks in Charleston, South Carolina. He has performed large-scale network security engineering for numerous government clients. His most recent work involves the Department of Defense medical community, where his team is responsible for the security posture of all Navy and Army hospitals and clinics in the world. His specialty is in purpose-built intrusion detection/protection, VPN encryption, firewall, content filtering, and secure remote access devices. His prior jobs include network engineering design, modeling, and testing for the Department of State, and pre- and post-sales network engineering for several optical/WAN vendors (Corvis Corporation, Corrigent Systems, Lucent Technologies, Ascend Communications, and Network Equipment Technologies). He holds a Master of Science degree in Electrical Engineering from George Washington University, and a Bachelor of Science degree in Mechanical Engineering from the University of Virginia. He holds a Top Secret/SCI clearance and is an IEEE member. Greg Miles (CISSP, CISM, IAM/IEM) is a co-founder, President, Chief Financial Officer, and Principal Security Consultant for Security Horizon, Inc., a Colorado-based professional security services and training provider and veteran-owned small business. He is a United States Air Force veteran and has served in military and contract support for the National Security Agency, Defense Information Systems Agency, Air Force Space Command, and NASA supporting worldwide security efforts. Greg has planned and managed Computer Incident Response Teams (CIRTs), Computer Forensics, and INFOSEC training capabilities. Greg has been published in multiple periodicals, including The Security Journal and The International Journal on Cyber Crime. He co-authored Network Security Evaluation: Using the NSA IEM (Syngress. ISBN: 978-1597490351) and Security Assessment: Case Studies for Implementing the NSA IAM (Syngress. ISBN: 978-1932266962). Greg is a network security instructor for the University of Advancing Technology (UAT) and an advisor with Colorado Technical University (CTU). Ed Fuller (CISSP, IAM/IEM) is Senior Vice President, COO, and Principal Security Consultant for Security Horizon, Inc. He has more than 28 years of experience in operations, communications, computer information systems, and security. He is the primary lead for INFOSEC Assessments and Training for Security Horizon. Ed has served as team lead for INFOSEC assessments for more than nine years. He has served other

companies as an INFOSEC Training Manager and Senior Security Consultant. Ed was integrally involved in establishing, implementing, and supporting the worldwide security program for the Defense Information Systems Agency (DISA), directly supporting Field Security Operations (FSO). He was a participant in the development of the Systems Security Engineering Capability Maturity Model (SSE-CMM) and has been a key individual in the development and maintenance of the Information Assurance Capability Maturity Model (IA-CMM). Ed also serves as a Lead Instructor for the National Security Agency (NSA) INFOSEC Assessment Methodology (IAM) and the INFOSEC Evaluation Methodology (IEM). Ed retired from the United States Navy with more than 23 years of distinguished service. Ed is a co-author for Security Assessment: Case Studies for Implementing the NSA IAM (Syngress. ISBN: 978-1932266962) and Network Security Evaluation: Using the NSA IEM (Syngress. ISBN: 978-1597490351) and a frequent contributer for the The Security Journal, a quarterly security periodical. Chris Hurley (IAM/IEM) is a senior penetration tester working in the Washington, D.C. area. He is the founder of the WorldWide WarDrive and organized the DEF CON WarDriving Contest from its inception until last year. He has authored or co-authored several books on wireless security and penetration testing, including WarDriving Wireless Penetration Testing (Syngress. ISBN: 978-1597491112), The Penetration Testers Open Source Toolkit (Syngress. ISBN: 978-1597490214), InfoSec Career Hacking (Syngress. ISBN: 978-1597490115), and Stealing the Network: How to Own an Identity (Syngress. ISBN: 978-1597490061). Rob Cameron (JNCIS-FWV, JNCIA-M, CCSP, CCSE+) is a Security Solutions Engineer for Juniper Networks. He currently works on designing security solutions for Juniper Networks that are considered best-practice designs. Rob specializes in network security architecture, firewall deployment, risk management, and high-availability designs. His background includes six years of security consulting for more than 325 customers. He is the lead author of Configuring Netscreen and SSG Juniper Firewalls (Syngress. ISBN: 978-1597491181) and Configuring NetScreen Firewalls (Syngress. ISBN: 978-1932266399). Brian Kirouac (CISSP, IAM/IEM) is the Chief Technology Officer and Principal Security Consultant for Security Horizon, Inc. Brian has more than 15 years of experience as an IT professional. Before joining Security Horizon, he served in a wide range of information technology positions in both domestic and international environments. He was a network administrator for a major university, eventually migrating to system administrator specializing in UNIX and Windows integration. He was also the Lead Technical Security Specialist at a municipal four-service utility. In addition to his current position at Security Horizon, Brian serves as an instructor for the National Security Agency (NSA) INFOSEC Assessment (IAM) and INFOSEC Evaluation (IEM) Methodologies and team member of NSA IA-CMM Appraisals. Brians publication history includes being a frequent contributor to The Security Journal, being both a refereed and invited speaker for SANS, and a refereed presenter for a NASA Conference on tethered satellites.