

About the Authors

Stephen Northcutt is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer. Stephen is author/co-author of *Incident Handling Step by Step*, *Intrusion Signatures and Analysis*, *Inside Network Perimeter Security*, and the previous two editions of this book. He was the original author of the Shadow intrusion detection system and leader of the Department of Defense's Shadow Intrusion Detection team before accepting the position of Chief for Information Warfare at the Ballistic Missile Defense Organization. Stephen currently serves as Director of Training and Certification for the SANS Institute.

Judy Novak is currently a senior security analyst working for the Baltimore-based consulting firm of Jacob and Sundstrom, Inc. She primarily works at the Johns Hopkins University Applied Physics Laboratory where she is involved in intrusion detection and traffic monitoring and Information Operations research. Judy was one of the founding members of the Army Research Labs Computer Incident Response Team where she worked for three years. She has contributed to the development of a SANS course in TCP/IP and written a SANS hands-on course, "Network Traffic Analysis Using tcpdump," both of which are used in SANS certifications tracks. Judy is a graduate of the University of Maryland—home of the 2002 NCAA basketball champions. She is an aging, yet still passionate, bicyclist, and Lance Armstrong is her modern-day hero!