Introduction To Network Security
(Chapman & Hall/CRC Computer And Information Science Series)
Unlike data communications of the past, today’s networks consist of numerous devices that handle the data as it passes from the sender to the receiver. However, security concerns are frequently raised in circumstances where interconnected computers use a network not controlled by any one entity or organization. Introduction to Network Security examines various network protocols, focusing on vulnerabilities, exploits, attacks, and methods to mitigate an attack. The book begins with a brief discussion of network architectures and the functions of layers in a typical network. It then examines vulnerabilities and attacks divided into four categories: header-, protocol-, authentication-, and traffic-based. The author next explores the physical, network, and transport layers of each network as well as the security of several common network applications. The last section recommends several network-based security solutions that can be successfully deployed.

This book uses a define-attack-defend methodology for network security. The author briefly introduces the relevant protocols and follows up with detailed descriptions of known vulnerabilities and possible attack methods. He delineates the threats against the protocol and presents possible solutions. Sample problems and lab experiments based on the concepts allow readers to experiment with attacks and assess the effectiveness of solutions. Two appendices provide further clarification and a companion website is offered which supplements the material. While most of the books available on this subject focus solely on cryptographic techniques to mitigate attacks, this volume recognizes the limitations of this methodology and considers a wider range of security problems and solutions. By focusing on a practical view of network security and examining actual protocols, readers can better understand the vulnerabilities and develop appropriate countermeasures.
This is an absolutely excellent book. It breaks down the basic network layers, their headers and their functions in an easy to understand format. It is not overly verbose and provides just the right amount of examples to give the reader a good understanding of how everything works and fits together. It also provides a good "taxonomy," as the author calls it, for classifying the attacks/mitigation techniques that can be implemented for the different network layers. Lastly and probably most importantly the book is written for some who has no knowledge of computer networking. It does and wonderful job of explaining things leaving the reader with an outstanding understanding of that subject.

Required for a class, but not very useful. Material has inaccuracies, isn't well presented, and unoriginal.

This book was alright. I took a class by this professor and used a draft of the final version of this book. The draft had a few inaccuracies, but that's why it was a draft, I would assume the issues are fixed now. The professor does know his stuff, but you should note that is is an introduction to network and general security. If your new to security and you want to learn a good "taxonomy" for network attacks then this is a good place to start, but I've seen better books on security. There are not many real world examples in this book because it is an introduction and it is assumed the skill set is not there yet, also because real world attacks change very quickly. The assignments recommended in this book are good and the accompanying code on the website is a good starter for getting interested in network security. However if you have any sort of network security experience already I would recommend diving into other books instead.

Download to continue reading...
Introduction to Network Security (Chapman & Hall/CRC Computer and Information Science Series)

Dmca