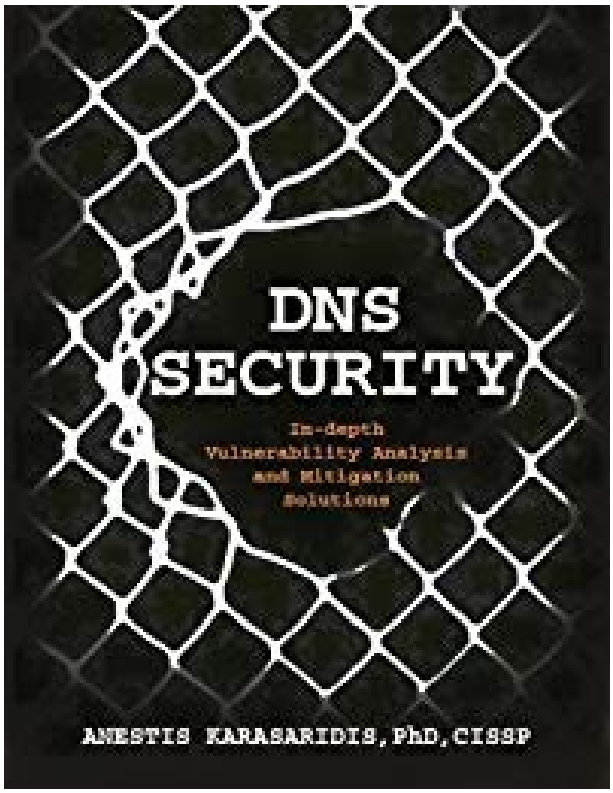
DNS Security: In-depth Vulnerability Analysis and Mitigation Solutions



Goodreads Rating:	4.17
ASIN	B007ZW50WE
Genre:	Uncategorized
Author:	Anestis Karasaridis
Published:	May 2nd 2012

The Domain Name System (DNS) is arguably one of the most important network infrastructure services. As the enabler of almost every web, email, instant messaging, and e-commerce transaction, it is the central nervous system of the Internet. DNS is also a critical component for new and emerging applications such as Voice over LTE (VoLTE) in cellular networks, Voice over IP (VoIP) Telephony, Radio Frequency IDs (RFID), and Content Distribution Networks (CDN). Now in IEEE ComSoc's Best Readings, this book gives the reader an in-depth understanding of how DNS works, its security vulnerabilities, how to monitor and detect security related events and how to prevent and mitigate attacks. After reading the book, the reader will be able to recognize and explain the major issues around DNS security, and know the best practices to setup, operate, and protect DNS service. This book provides a comprehensive coverage of DNS security and is mainly addressed to Information Systems security professionals such as network and system analysts and administrators, network and security operations personnel, network designers and architects, as well as the research community. Sections of the book can be used as assigned reading for undergraduate or graduate classes in network/application security. The book is organized in six chapters. Chapter 1 gives an introduction to the topic, illustrating the importance of DNS Security and providing the motivation for in-depth study of the topic. Chapter 2 gives a comprehensive overview of the protocol, common service architectures, and most common applications using DNS. In Chapter 3, we describe security vulnerabilities at the architectural, protocol, configuration and implementation levels. In Chapter 4, we review how to monitor DNS traffic in different environments and examine techniques to detect security related events. Chapter 5 examines how to prevent, protect against and mitigate attacks. Finally, in Chapter 6 we examine in detail the DNSSEC protocol and its implementation. We conclude examining DNSCurve, an alternative proposal for securing DNS

transactions. Awarded IEEE Communication Society's best readings (Books category)