Review of the book

"Cyber Security Essentials"

by James Graham, Richard Howard and Ryan Olson

CRC Press, Taylor & Francis Group, 2011

ISBN: 978-1-4398-5123-4

Dr. Emin İslam Tatlı
Daimler TSS

June 2013

1 Summary of the review

Reading the title of the book, one might expect that it would focus on past, today and future of cyber security and cyber wars as well as its social aspects. This was at least my expectation. But the book is a very classical network security book and provides only technical details about various security issues.

On the other hand, the book delves into important network security aspects and provides valuable information. Reading the book, you will learn about

- fundamentals of network security including DNS security, Firewalls, Virtualization
- attacker techniques (e.g. proxies, tunneling, fraud techniques)
- exploiting including shellcodes, application-level injections, race conditions, malicious PDF files
- malicious codes including viruses, worms, rootkits, spyware, privilege escalation, DLL injection etc.
- defense techniques with honeypots and automated code analysis systems

In this review, I will summarize the chapters, provide positive and negative aspects of the book and define the target readership from my perspective.

2 Summary of the book

The book is divided into 5 chapters. The following will summarize the content of each chapter and give an overview of the book.

- **Chapter 1 - Cyber Security Fundamentals:** This chapter begins with fundamentals of security (i.e. authentication, authorization, nonrepudiation, confidentiality, integrity and availability). Symmetric encryption, DNS security, firewalls, virtualization security and Microsoft Windows security principles are further topics that are explained within this chapter.
- **Chapter 2 - Attacker Techniques and Motivations:** Using proxies as attacking tools, tunneling techniques, phising, mobile malicious code, click fraud and botnets are the topics of this chapter.

- **Chapter 3 - Exploitation:** Buffer overflows, format string vulnerabilities, SQL injection, Cross Site Scripting, malicious PDF files, race conditions, Denial of Service, brute force and dictionary attacks and social engineering are explained in this chapter.
- **Chapter 4 - Malicious Code:** This chapter explains malicious code (e.g. viruses, worms), rootkits, spyware, security aspects of BIOS/CMOS/MBR, man in the middle attacks, DLL injections and security implications of browser helper objects.
- **Chapter 5 - Defense and Analysis Techniques:** Memory forensics, honeypots and automated malicious code analysis systems are explained in details within this chapter.

3 What is the book like (style)?

The book is a technical book focusing mainly on network security. It explains some aspects of application security, but only in a very limited way. As an example, SQL injection is summarized in 3 pages without explaining different types of SQL injection. On the other hand, the mentioned network security topics are explained in details with attack techniques and required countermeasures.

Regarding the style, the book is not very structured and not arranged in a good logical order. Various security topics are put together and distributed in different chapters. It is not easy to follow the relation and order of different chapters.

4 Would you recommend this book?

From my point of view, putting all these together, I would recommend this book only to network security experts who need to understand the technical details of certain topics like malicious code and network exploitation techniques. Otherwise, this book is suitable neither for application security experts nor for students.

The reviewer is working as IT-Security Architect and Researcher by Daimler TSS (Technologies, Services, Solutions) in Germany.