The Homepage of @attrc

Home

Recommended Reading

This page lists books that I have found to be highly relevant and useful for learning topics within computer security, digital forensics, incident response, malware analysis, and reverse engineering. These books range from introductory texts to advanced research works. While some of these books may seem dated, the information contained is still very useful to people learning today, and much of the information is essential to becoming proficient in the information security realm.

Please note that, in order to avoid ranking individual books, each category is listed in alphabetical order and each book is listed in alphabetical order within its category.

If you notice any errors with this page or have books that you think should be listed then please contact me. I will only list books that I have personally read and for which I am willing to vouch.

Application Security - Native

Title	Comments	Technical Level
The Art of Software Security Assessment	The Bible of source code auditing	Intermediate-Advanced. Ability to read C/C++ required to get full value.
Secure Coding in C and C++	Arguably the best text for writing secure low-level code	Accessible to all that can read/write C and C++

Application Security - Web

Title	Comments	Technical Level
The Browser Hacker's Handbook	Written by the authors of BeEF. A detailed look into many web security topics	Covers basic through advanced topics
The Database Hacker's Handbook	The most detailed book available for attacking databases	Covers basic through advanced topics
The Tangled Web	A detailed look at the foundations of web protocols followed by a thorough examination of their weakness. Highly, highly recommended	Accessible to all. The beginning chapters cover background needed for later advanced topics
The Web Application Hacker's Handbook	Covers a wide range of web security issues	Intermediate

Cryptography

Title	Comments	Technical Level
Applied Cryptography	The standard for learning cryptography	Ranges from background and introduction to deep algorithms and security considerations
Introduction to Modern Cryptography	A well-done, formal look at cryptography. Used in many graduate level computer science programs	Advanced - full understanding requires deep mathematical knowledge

Database Forensics

Title	Comments	Technical Level
Microsoft SQL Server Internals	Examination of MSSQL akin to the OS-level examination of Windows Internals	Intermediate - learn database basics before reading
SQL Server Forensic Analysis	A deep look at forensic analysis of MSSQL Systems	Intermediate - learn database basics before reading

Digital Forensics and Incident Response

Title	Comments	Technical Level
File System Forensic Analysis	The definitive resource for file system forensics	Intermediate-Advanced

Forensic Discovery	A foundational text of computer forensics by two of the earliest pioneers	Intermediate
Real Digital Forensics	A concise introduction to forensic processes	Beginner-Intermediate
Windows Forensic Analysis, Second Edition	This book, along with the 4th edition, are the best books available for Windows disk forensics	Ranges from basic concepts to advanced analysis
Windows Forensic Analysis, Fourth Edition	This book, along with the 2nd edition, are the best books available for Windows disk forensics	Ranges from basic concepts to advanced analysis

Exploitation / Penetration Testing

Title	Comments	Technical Level
A Guide to Kernel Exploitation	Advanced exploitation of a range of operating systems	Advanced
Android Hacker's Handbook	A deep dive into exploitation of Android systems	Intermediate
Hacking: The Art of Exploitation, 1st Edition	A foundational work of low-level exploitation	Intermediate
iOS Hacker's Handbook	A deep dive into exploitation of iOS devices	Intermediate-Advanced
The Mac Hacker's Handbook	A deep dive into exploitation of Mac systems	Intermediate-Advanced
Rtfm: Red Team Field Manual	A concise, well written guide that should be in every penetration tester's travel bag	Accessible to all people with a pen test background
The Shellcoder's Handbook	Crafting shellcode and exploits	Intermediate-Advanced

Linux Usage

Title	Comments	Technical Level
Linux in a Nutshell	The best text to learn how to use Linux	Beginner-Intermediate
Running Linux	Another great text from which to learn Linux	Beginner-Intermediate

Malware Development and Analysis

Note: Many of these books contain information related to Reverse Engineering

Title	Comments	Technical Level
The Art of Computer Virus Research and Defense	A deep look at many facets of malware analysis	Intermediate
Malware Analyst's Cookbook	A "recipe" approach to many topics in malware analysis	Intermediate-Advanced
Malware Forensics	A well done introduction to malware analysis	Beginner
Practical Malware Analysis	A very approachable book to many topics in malware analysis	Intermediate
Rootkits: Subverting the Windows Kernel	A study of many rootkit techniques still in use today	Intermediate-Advanced
The Rootkit Arsenal	An 800 page epic of rootkit development and analysis	Intermediate-Advanced

Memory Forensics

Title	Comments	Technical Level
The Art of Memory Forensics	A 900 page exploration of memory forensics across the major operating systems. NOTE: I am a co-author of this book	Ranges from introductory material to advanced analysis
What Makes It Page?	A deep look into the Windows memory manager	Intermediate

Network Forensics

Title	Comments	Technical Level
The Practice of Network Security Monitoring	Beyond just packet analysis to how to integrate network forensics into a real world environment	Intermediate
Practical Packet Analysis	An excellent resource for learning to identify and analyze network traffic	Beginner-Intermediate
Wireshark (R) 101	A deep exploration of Wireshark	Beginner-Intermediate

Networking

Title	Comments	Technical Level/th>
CCNA Cisco Certified Network Associate Study Guide	A primer on real world networking and networks	Intermediate
CompTIA Network+ All-In-One Exam Guide	An essential book for those looking to learn networking	Beginner
TCP/IP Illustrated	The Bible of networking protocols. A must read	Intermediate

Operating Systems Internals - General

Title	Comments	Technical Level
Intel Architecture Manuals	Very well done documentation on the hardware architecture. Free to download	Intermediate-Advanced
Modern Operating Systems	The classic dinosaur book from Tanenbaum	Intermediate-Advanced

Operating Systems Internals - Linux

Title	Comments	Technical Level
Linux Device Drivers, 3rd Edition	Best resource to learn Linux's driver architecture	Intermediate-Advanced
Linux Kernel Development, 3rd Edition	Rob Love on programming in the Linux kernel	Intermediate-Advanced
The Linux Programming Interface	Excellent book on programming the Linux environment	Intermediate-Advanced
Understanding the Linux Kernel, Third Edition	The equivalent of Windows Internals for Linux	Intermediate-Advanced

Operating Systems Internals - Mac

Title	Comments	Technical Level
Mac OS X Internals: A Systems Approach	Windows Internals for Mac	Intermediate-Advanced
Mac OS X and iOS Internals	Read this after reading Mac OS X Internals	Intermediate-Advanced

Operating Systems Internals - Windows

Title	Comments	Skill Level
Windows Internals	Read this book if you want to understand Windows	Intermediate-Advanced
Windows System Programming (4th Edition)	A step-by-step guide through the Windows API	Intermediate

Programming - Concepts and Algorithms

Title	Comments	Technical Level
Compilers: Principles, Techniques, and Tools	The famous dragon book on compilers	Advanced - Don't read until you have a solid understanding of programming and runtime environments
Design Patterns	Required reading for any serious programmer	Intermediate
Linkers and Loaders	Required reading for understanding program linking and runtime loading	Intermediate

Programming - Language Specific

Note: The reason there are few books here is due to languages having amazing learning resources online

Title	Comments	Technical Level
Advanced Programming in the UNIX(R) Environment	Deep exploration of programming related to Linux, Mac, and BSD	Beginner-Intermediate
The C Programming Language, 2nd Edition	"K and R" - required if you want to be proficient with C	Intermediate-Advanced
Violent Python	Learn Python programming and directly apply it to forensics	Basic to advanced topics

	and security	

Reverse Engineering

Title	Comments	Technical Level
Assembly Language Step-by-step	The best resource to learn assembly. Later books focused on "high level" assembly as opposed to actual instructions	Intermediate-Advanced
Hacker Disassembling Uncovered	A great resource for advanced topics in reverse engineering	Intermediate-Advanced
Hacking the Xbox	A well written and fun book from which to learn reversing	Intermediate
The IDA Pro Book	The best resource to learn IDA	Intermediate
Reversing: Secrets of Reverse Engineering	One of my favorite books. A chapter is dedicated to reversing a Windows API back to C so perfectly that compiling it matches the hash of the Windows DLL	Intermediate-Advanced
Practical Reverse Engineering	Reversing across Intel and ARM	Intermediate

Tradecraft - Digital

Title	Comments	Technical Level
Silence on the Wire	lcamtuf's exploration of vulnerabilities and attacks that most people would never think of. Strongly recommended	Beginner-Advanced

Tradecraft - Traditional

Note: I originally found several of these books from The Grugq's list

Title	Comments	Technical Level
The Art of Intelligence	Tradecraft and real-world analysis from Henry Crumpton	Beginner-Intermediate
Chinese Intelligence Operations	A well-written, deep study of Chinese intelligence services	Advanced
See No Evil	Tradecraft and lessons from a former CIA analyst in the Middle East	Intermediate
Spy Handler: Memoir of a KGB Officer	Written by the KGB officer whom handled Robert Hanssen and Aldrich Ames. A great text to learn real world tactics and techniques	Beginner-Intermediate
Terrorism and Counterintelligence: How Terrorist Groups Elude Detection	A deep examination of modern terrorist groups and counterintelligence use	Intermediate
Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer	Read this first - a textbook on how to be a counter intel officer along with terms, techniques, and tactics	Beginner - make this your first book