Piracy is your friend

Cybersecurity - Livello Fondamentale

1. "Cybersecurity for Beginners" - Raef Meeuwisse

- **Focus**: Introduzione completa ai concetti base
- **Perché leggerlo**: Linguaggio accessibile, copertura completa dei foundation concepts
- **Argomenti**: CIA triad, threat modeling, risk management, governance

2. "The Web Application Hacker's Handbook" - Dafydd Stuttard, Marcus Pinto

- **Focus**: Sicurezza applicazioni web
- **Perché leggerlo**: Standard de facto per web security, approccio metodologico
- **Argomenti**: OWASP Top 10, injection attacks, authentication bypass, session management

3. "Network Security Essentials" - William Stallings

- **Focus**: Sicurezza di rete e crittografia
- **Perché leggerlo**: Approccio matematico rigoroso, copertura teorica e pratica
- **Argomenti**: Symmetric/asymmetric cryptography, PKI, IPSec, TLS/SSL

Cybersecurity - Livello Avanzato

4. "Advanced Penetration Testing" - Wil Allsopp

- **Focus**: Tecniche avanzate di penetration testing
- **Perché leggerlo**: Va oltre i tool automatici, focus su metodologie custom
- **Argomenti**: Advanced persistence, evasion techniques, custom exploit development

5. "The Shellcoder's Handbook" - Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte

- **Focus**: Exploit development e reverse engineering
- **Perché leggerlo**: Comprensione profonda delle vulnerabilità a livello assembly
- **Argomenti**: Buffer overflows, heap exploitation, return-oriented programming

6. "Practical Malware Analysis" - Michael Sikorski, Andrew Honig

- **Focus**: Analisi e reverse engineering di malware
- **Perché leggerlo**: Approccio hands-on con laboratori pratici
- **Argomenti**: Static/dynamic analysis, debuggers, disassemblers, behavioral analysis

Social Engineering

7. "The Art of Human Hacking" - Christopher Hadnagy

- **Focus**: Framework completo di social engineering
- **Perché leggerlo**: Approccio sistematico basato su psicologia cognitiva
- **Argomenti**: OSINT, pretexting, influence principles, elicitation techniques

8. "Ghost in the Wires" - Kevin Mitnick

- **Focus**: Autobiografia del più famoso social engineer
- **Perché leggerlo**: Esempi reali di tecniche di manipulation, narrative engaging
- **Argomenti**: Phone phreaking, dumpster diving, insider manipulation

9. "Social Engineering: The Science of Human Hacking" - Christopher Hadnagy

- **Focus**: Aspetti scientifici e psicologici del social engineering
- **Perché leggerlo**: Foundation teorica solida basata su ricerca empirica
- **Argomenti**: Cognitive biases, psychological triggers, influence psychology

Incident Response e Forensics

10. "The Practice of Network Security Monitoring" - Richard Bejtlich

- **Focus**: Network security monitoring e threat hunting
- **Perché leggerlo**: Metodologia per detection e response sistemica
- **Argomenti**: NSM theory, traffic analysis, indicator development

11. "Incident Response & Computer Forensics" - Jason T. Luttgens, Matthew Pepe, Kevin Mandia

- **Focus**: Metodologie di incident response
- **Perché leggerlo**: Approccio enterprise-grade per IR
- **Argomenti**: IR lifecycle, evidence collection, timeline analysis, reporting

12. "File System Forensic Analysis" - Brian Carrier

- **Focus**: Digital forensics a livello file system
- **Perché leggerlo**: Comprensione tecnica profonda dei file systems
- **Argomenti**: NTFS, EXT, FAT analysis, deleted file recovery, timeline construction

Crittografia e Sicurezza Teorica

13. "Cryptography Engineering" - Niels Ferguson, Bruce Schneier, Tadayoshi Kohno

- **Focus**: Implementazione pratica di sistemi crittografici
- **Perché leggerlo**: Bridge tra teoria crittografica e implementazione sicura
- **Argomenti**: Protocol design, side-channel attacks, key management

14. "Security Engineering" - Ross Anderson

- **Focus**: Progettazione di sistemi sicuri
- **Perché leggerlo**: Visione sistemica della security, casi di studio reali
- **Argomenti**: Security models, access control, distributed systems security

Governance e Management

15. "CISSP All-in-One Exam Guide" - Shon Harris

- **Focus**: Governance, risk management, compliance
- **Perché leggerlo**: Comprehensive coverage dei domini CISSP
- **Argomenti**: Security governance, BCP/DRP, legal and compliance issues

16. "Measuring and Managing Information Risk" - Jack Freund, Jack Jones

- **Focus**: Quantitative risk analysis (FAIR methodology)
- **Perché leggerlo**: Approccio quantitativo al risk management
- **Argomenti**: Risk quantification, Monte Carlo analysis, business impact

Specializzazioni Emergenti

17. "The Car Hacker's Handbook" - Craig Smith

- **Focus**: Automotive cybersecurity
- **Perché leggerlo**: Dominio emergente con unique challenges
- **Argomenti**: CAN bus analysis, ECU reverse engineering, vehicle network security

18. "IoT Penetration Testing Cookbook" - Aaron Guzman, Aditya Gupta

- **Focus**: IoT device security
- **Perché leggerlo**: Metodologie per testing di dispositivi embedded
- **Argomenti**: Firmware analysis, hardware hacking, wireless protocol security

19. "Practical Cloud Security" - Chris Dotson

- **Focus**: Cloud security architecture
- **Perché leggerlo**: Cloud-native security patterns e best practices
- **Argomenti**: Container security, serverless security, multi-cloud governance

Raccomandazioni per Percorso di Studio

Path per Principianti:

1. Cybersecurity for Beginners
2. Network Security Essentials
3. The Art of Human Hacking
4. Ghost in the Wires

Path per Tecnici:

1. The Web Application Hacker's Handbook
2. Practical Malware Analysis
3. The Shellcoder's Handbook
4. File System Forensic Analysis

Path per Manager/Governance:

1. Security Engineering
2. CISSP All-in-One Exam Guide
3. Measuring and Managing Information Risk
4. The Practice of Network Security Monitoring

Note Metodologiche:

- **Hands-on Practice**: Combina sempre la lettura con laboratori pratici
- **Community Engagement**: Partecipa a CTF, bug bounty programs, security conferences
- **Continuous Learning**: Il campo evolve rapidamente, mantieni aggiornamento costante

- **Specialization**: Dopo le basi, focalizzati su 2-3 domini specifici per expertise profonda