- Chapter 1:
  - 1: CIA, impact, challenges
  - 2: Assets, threats
  - 3: Attack surfaces, strategies
- Chapter 2: crypt
  - 4: block/stream cypher
  - 5: DES/AES
  - 6: Public-key requirements
  - 7: message authentication
  - 8: hash, random
- Chapter 3: User Authentication
  - 9: pass and salt
  - 10: shadow, cards
  - 11: biometric, multi-factor, remote authentication
  - 12: challenge-response, authentication security issues
- Chapter 4: Access Control
  - 13: policies
  - 14, 15: DAC, Unix, setuid, setgid, ACLs
  - 16: 17: RBAC, ABAC
- Chapter 5: Database and cloud security
  - 19: injection, database/SQL access control
  - 20: RBAC,
  - 20, 21: inference, database encryption
  - 22: cloud computing, cloud service models, NIST deployment models
- Chapter 6: malicious software
  - 23, 24: types, attack sources, advanced persistent threats (APTs),
  - 25, 26: viruses
  - 26, 27: worms, target, scanning, mobile code, drive-by-downloads, watering hole, **malvertising**
  - 28, 29: Spam, trojans, logic bomb, keylogger, spyware, **phishing**, bookdoor, rootkit, trojan payloads, bot
  - 30: generic decryption, host-based behavior block-software, perimeter scanning approches
- Chapter 7: DoS
  - 32: ping flood, backscatter, syn flooding
  - 33: DDoS, HTTP flood (spidering), Slowloriss, Reflection, delayed binding, load balancer
  - 34: DNS Amplification, DoS attack defenses, SYN Spoofing attack prevention
  - 35: responding to DoS Attacks
- Chapter 8: Intrusion Detection
  - 36: IDS, Comopnents, Requirements, analysis approaches, Anonaly Detection
  - 37: Host-based IDS, data sources and sensors
  - 37, 38: Network-based IDS
  - 38: Intrusion detection techniques, **suitability**, logging, AESS
  - 39: IETF Intrusion Detection Message Exchange, Honeypots, Snort IDS
- Chapter 9: Firewalls and Intrusion Prevention Systems
  - 40: Need, Characteristics, Access Policy, Firewall filter characteristics
  - 41: Pros and Cons, Filtering example
  - 42: Filter Pros and Cons, Attacks and measure, Stateful Inspection Firewall, IP address spoofing, source routing, tiny fragment

  - 43: Application-Level Gateway, Host-based firewalls, Personal Firewall, External & Internal Firewalls, VPN and IPSec
  - 44: Distributed Firewall, IPS, HIPS (host-based), Protection areas of HIPS, The Role of HIPS, Network-based IPS (NIPS)
  - 45: Snort Inline
- Chapter 10: Buffer overflow
  - 46: Concept, Attacks, Stack overflow
  - 47: Shell Code, Stack Overflow Variants, Defenses
  - 48: Stackguard, Stackfield, Compile-Time defenses, Stack Protection, Run-time, NC-bit, Address Space Layout Randomization, Guard Pages
  - 49: Heap Overflow, Global Data, Integer
- Chapter 13: Trusted Computing and Multilevel Security
  - 50, 51: BLP, Biba, CW
  - 52, 53: Reference Monitor, MLS for databases, write/read access, polyinstantiation
  - 54: TCB, TPM, Authenticated Boot Service
  - 54: Ceritifcation Service, Encryption Service, Critera,
- Meltdown: 55, Spectra: 61