Study Guide – Chapters 1-6

Chapter 1 – Overview
- Security concepts
- CIA triad
- Vulnerabilities, threats, and attacks
- Countermeasures
- Passive vs. active
- Security services
- Trends
- Strategy

Chapter 2 – Cryptographic tools
- Symmetric encryption
- Message authentication
- Public-key encryption
- Digital signatures
- Random / Pseudo random numbers

Chapter 3 – Authentication
- Types of authentication
- Password, tokens, biometric
- Remote user issues
- Authentication issues

Chapter 4 – Authorization
- Components of access control
- DAC
- MAC
- RBAC
- ABAC

Chapter 5 – Database security
- Relational databases
- SQL injection
- Access control wrt databases
- Inference
- Encryption
- No Cloud Security

Chapter 6 – Malware
- Types of Malware
- Life cycles of malware
- Types of propagation
- Types of payloads
- Countermeasures

Network
- Protocol stack
- Responsibility of IP
- Responsibility of TCP
- Connection vs. connectionless