Study Guide for CyberSecurity Comprehensive Exam

Recommended books:

- Conklin et al., Principles of Computer Security
- William Stallings, Cryptography and Network Security, Principles and Practices,
- Marie Wright and John Kakalik, Information Security-Contemporary Cases
- Simson Garfinkel, Web Security, Privacy and E-Commerce

Review Topics and Desired Learning Outcomes, grouped by area:

Security Architecture and Threats

1. Understand what constitutes OSI X.800 security model and ITU-T X.805 model
2. Understand kinds of security attacks, security mechanisms, and security services.
3. Understand the relationship between services and attacks, and between mechanisms and attacks.
4. Understand C(Confidentiality), I (Integrity) A (availability) and how CIA relates to security services, mechanisms and attacks.

Cryptography

1. Understand the types of attacks for cryptography.
2. Understand the basic substitution and transposition techniques, solve it by examples.
3. Understand the block cipher and stream cipher, the difference between two and the cipher algorithms that use them.
4. Understand what the link to link encryption and end to end encryption are.
5. Understand multiple encryptions, solve it by simple examples
6. Able to describe variants of 3-DES with two keys and three keys.
7. Able to describe what the Man-in-the-middle attack is. Understand why Diffie Hellman key exchange protocol is subject to the man in the middle attack.
8. Understand the meaning of each Block Cipher modes and their corresponding applications. Abbreviation of each mode. Like CBC and CFB, .etc.
9. Understand in high level how RC4 works, and what are the applications using RC4. Do you also know where DES might be used? Answer for DES is Governments, financial sectors, and VPN.
10. Understand the principles of public key cryptography and its six components.
11. Understand the differences between Asymmetric and Symmetric algorithms in terms of algorithms, efficiency, security, applications, .etc.
12. Describe RSA algorithm in high level, and know how to use it by examples shown in the slides and at the on-line session.
13. Understand DSS and ECC and their application.
14. Able to describe how Digital Signature works.

Authentication and email Security
1. Understand approaches to Message Authentications.
2. Understand how Kerberos works, its weakness, and its requirements.
3. Understand the differences between Kerberos 4 and 5.
4. Understand what X.509 is. What it does. Difference between version 2 and version 3?
5. Understand what PKI (public Key Infrastructure) is.
6. Summarize the PGP services (digital signature, encryption, compression, email compatibility and segmentation).
7. What is the key rings in PGP?
8. Describe the functions of S/MIME

**IP and Web Security**

1. Understand the functions of each SSL layer.
2. Able to list three functional areas of IPsec, and describe applications of IPsec.
3. Understand services, able to identify which protocols (AH, ESP only and ESP with authentication) provides which service(s).
4. Able to identify services provided by IPsec and key management schemes used by IPsec.
5. Understand the difference between IPsec tunnel mode and transport mode.
6. Understand how to combine security association with two ways: transport adjacency and iterated tunneling.

**Intrusion Detection and Password Management**

1. Identify three types of intruders
2. Identify two approaches of intruder detection (Statistical anomaly detection) and Rule-based detection.
3. Understand the relationship among measures, models, and detected intrusions.
4. Understand the concepts of honeypot why it is needed?
5. Able to list at least two password selection strategies

**Firewall Design**

1. Understand 4 general techniques that firewall uses to control access and enforce its site’s security.
2. What attacks can be made to packet filtering firewall.
3. Understand Access control matrix model and Bell La-Padula model.
4. What is capability table and access control list? Row or column in the access matrix.
5. Understand different types of firewall, packet filtering, application proxy, and circuit level gateway.
6. What is stateful inspection firewall and how it differs from traditional packet filtering?

**Malicious Software**

1. Understand the meaning of each type of malicious software, like virus, worm, Trojan horse, .etc... And identify if host program is required to launch an attack?
2. Understand approaches taken by antivirus software, advanced technology, and their generations.
3. Describe DDoS attack methods; examples like Distributed SYN flood and Distributed ICMP attack. What are countermeasures of DDoS?
4. Understand 4 generations of virus countermeasures, and two advanced antivirus techniques (Generic Decryption and Digital Immune System.)

Business Continuity
1. Know the ways a company can protect personal data of its employees.
2. Know the types of encryption systems available (asymmetric and symmetric) and how key management works. Be able to give examples of systems.
3. Know the ways a company can protect itself in terms of physical security with examples.
4. Be able to list the elements of the US infrastructure and how they can be attacked.
5. Be able to list items regarding disaster recovery planning for a company. Planning, testing, locations of backup facilities, types of facilities.
5. Describe at least two examples of applications that uses IPsec. For each of example, state whether transport mode or tunnel mode is used, and why?