|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lecture Slides** | **Topic** | **Keywords** | **Ref Book chapter (Comp TIA)** | **Pages** |
| 2 | General Security Concepts | Information security triad, Access control, Authentication | Chapter 1: General Security Concepts |  |
| 3 | Identifying potential Risks | Attack strategies, Types of Attacks (DDOS, Man-in-the middle) | Chapter 2: Identifying potential Risks |  |
| 4 | Attack methods | TCP/IP security concerns (UDP attacks), Software exploitation, Surviving Malicious codes (Viruses, Worms, Trojan horses) | Chapter 2: Identifying potential Risks |  |
| 5 | Cryptography Basics | Physical Cryptography, Vignere Cipher, Caesar cipher | Chapter 7: Cryptography Basics, Methods, and Standards |  |
| 6 | Cryptography Methods and standards | Symmetric Algorithms (DES), Asymmetric Algorithms (Public private key), PKI | Chapter 7: Cryptography Basics, Methods, and Standards |  |
| 7 | Security Policies and Procedures | Business continuity, Disaster recovery, Alternate sites, Backups | Chapter 8: Security Policies and Procedures |  |
| 8 | Defense in Depth | Attacks and defenses, Implementing access controls, Perimeter security, Security zones, Biometrics, Social engineering | Chapter 6: Securing the Network and Environment |  |
| 9 | Hardening Systems | Hardening the OS and NOS, Network binding (NetBEUI), Hardening file systems (NTFS, FAT) | Chapter 5: Implementing and Maintaining a Secure Network |  |
| 10 | Firewall and Intrusion Detection Systems | Firewalls (Packet, Proxy), Intrusion Detection and Prevention principles, Common detection methodologies | Chapter3: Infrastructure and Connectivity |  |
| 11 | Secure software Development | In defensive programming, SDLC |  |  |