Not tested:

* Fire wall
* Encryption detection
* AES – (not the algo but symm and asymm encryption)
* DES - (not the algo but symm and asymm encryption)

Topics to focus on:

* **Information security**
  + **Security level**
  + **Goals (Confidentiality, Integrity, Availability) (Authentication, Privacy, Non-repudiation)**
* **Attacks on information security and security threats**
  + **Social engineering and phishing attacks. Different types, methods and role of social networking sites.**
  + **Credit card and identity theft**
  + **Password and pin cracking**
* Security Planning
  + **Two aspects** of information security (**technical and managerial**)
  + Security approaches (**bottom-up, top-down**)
    - **Bottom-Up: Never succeeds**
    - **Top-Down: Is recommended because:**
      * Clear Policy, Adequate Budget, Consistent support and procedures to protect hardware, software and other computer-based resources
* **DLM Model: Four tiers**, why top management support is important and how the support should be demonstrated by the top management.
  + Why **security just based on policy or technology will fail**?
  + **What is required** for secure system (**Both Policy and Technology**).
* **Cryptography**
  + Encryption and decryption **process**, how **encryption provides security** and types of encryptions (**symmetric and asymmetric**)
  + **Role of a key length**
  + **Substitution cipher** (**Mono and Poly substitution ciphers**), **additive cipher**
    - **Calculation: Encryption and decryption using additive cipher**
* **Secret key cryptography** (Concepts, advantages and disadvantages)
* **Public key cryptography** (Concepts, advantages and disadvantages)
* **RSA**
  + The **algorithm, key generation (e and d), encryption, decryption, authentication, security, advantages, disadvantages.**
  + **Calculations: encrypt and decrypt message, sign and verify message (digital signature using RSA).**
* **Digital Signatures** (Authentication, Nonrepudiation)
  + How it works, digital certificates, **CA, how to verify** the digital signature and **digital certificates**, what aspects of security does digital signature offer, how it offers authentication and non-repudiation, **RSA-based digital signature**.
* **Diffie-Hellman Key Exchange Algorithm**
  + The algorithm**, reasons behind its development, how it works**, show **how the sender and receiver will receive the same key without compromising the security.**
  + **Calculations**: Detailed **Calculation of public and shared secret keys**
* **Authentication and Authorization**
  + Difference between Authentication and Authorization
  + Can Authorization be allowed without Authentication
* **Hashing**
  + How it provides integrity. **Difference between encryption and hashing. Can we un-hash a sequence?**
* **SSL and SET (WEB Security) Protocols**
  + Differences, properties, advantages and disadvantages
  + **SSL and TLS 1.3 handshake protocol (Ephemeral Diffie-Hellman)**
  + How does **SET provide consumer and merchant authentication**.
  + SET and SSL use same technology then, **why SET failed and SSL became standard for web security.**
* **Password-Based Security** 
  + **Advantages and disadvantages of password-based authentication.**
  + **Calculations**: How long it will take to crack a password
  + Role of **special characters** and **small** and **capital letters** (make password strong)
  + **Password selection and implementation policies and why it is difficult to enforce it.**
  + Why shouldn’t one use the **same password for different web sites?**
* DOS
  + **Basic concepts of Denial of Service (Dos) and DDOS** (distributed denial of service) attacks.
  + **Common Protections** against DOS attacks
  + **SYN flood attack, how it works and how it can be launched.**
  + **Calculations**: how many **packets** are required to launch a DOS attack
  + What is the **impact of the packet size**
  + **How the speed of the link affects the DOS attack**
  + **Disadvantages of DoS attack**