1. Ethical hacking
2. CIA: Confidentiality, Integrity, Availability
    a. Concepts,
    b. Tools, encryption, access control, checksum, redundancy,
3. AAA: Authenticity, Assurance, Anonymity
    a. Digital signature, nonrepudiation, Proxies, Aggregation,
4. Threats and Attacks
    a. Eavesdropping, Alteration, DOS, Masquerading, Repudiation, Correlation, traceback,
5. Security principles
6. Encryption and Decryption
    a. Symmetric vs public-key
    b. Key management
    c. Hash functions
    d. MAC: message authentication code
    e. Digital Certificates
    f. Password: Brute Force Test
7. OS Security
    a. Processes
    b. File Systems, permissions
    c. Memory organization
    d. BIOS,
    e. Memory and Filesystem Security
    f. Password Salt
    g. Buffer overflow, stack vs. heap, Canary
    h. Shellcode Injection
8. Malware
    a. Insider attacks, Backdoors, Logic Bombs
    b. Defenses against insider attacks
    c. Virus: encrypted, polymorphic, metamorphic
    d. Worms, Trojan Horses, Rootkits, Zombies,
    e. Adware, Spyware
    f. Malware Countermeasure: signatures, not the digital signature
    g. White/black listing with hash
9. Network Security
    a. Packet switching: best effort, network layers, protocols,
    b. Data link layer, MAC, ARP, ARP Spoofing, ARP Caches, Poisoned ARP caches,
    c. Network layer: IP address, routing, ICMP attacks, Smurf attack, IP vulnerabilities, IP traceback,
    d. Transport layer: TCP, sequence number, port, SYN flood, Congestion control, Optimistic ACK attack, Session hijacking, IP spoofing, packet sniffer, Port Knocking, UDP, NAT
10. Denial-of-Service Attacks: ICMP attacks, smurf attack, SYN Flood attack, Optimistic TCP Attack, DDOS, IP traceback
11. DNS: Recursive Name resolution, Iterative Name Resolution, DNS Hijacking, DNS Cache Poisoning,

12. Firewalls: stateless vs. stateful, Tunnels, VPN, Intrusion Detection Systems, IDS Base-Rate Fallacy, Rule-based vs. statistical
13. Wireless: Hidden Terminal Problem, WEP, IP Redirection attack, authentication spoofing, WPA
14. Web: Phishing, ActiveX vs. Java, Cookies, Cross Site Scripting (XSS), XSS attack, SQL Injection
15. BlockChain: peer-to-peer electronic cash system, Bitcoin authentication, Bitcoin Integrity, hashing, chain of digital Signatures
16. Cryptography: symmetric, substitution cipher, one-time pads, block cipher, DES, AES, block cipher modes, ECB, CBC, stream cipher, public key encryption, GCD, relatively prime, modular, RSA,
17. Digital Signature, Message Authentication Code (MAC)