Test2 Study Guide:

1. Denial-of-Service Attacks: ICMP attacks, smurf attack, SYN Flood attack, Optimistic TCP Attack, DDOS, IP traceback
2. DNS: Recursive Name resolution, Iterative Name Resolution, DNS Hijacking, DNS Cache Poisoning,
3. Firewalls: stateless vs. stateful, Tunnels, VPN, Intrusion Detection Systems, IDS Base-Rate Fallacy, Rule-based vs. statistical
4. Wireless: Hidden Terminal Problem, WEP, IP Redirection attack, authentication spoofing, WPA
5. Web: Phishing, ActiveX vs. Java, Cookies, Cross Site Scripting (XSS), XSS attack, SQL Injection
6. BlockChain: peer-to-peer electronic cash system, Bitcoin authentication, Bitcoin Integrity, hashing, chain of digital Signatures
7. 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,