CompTIA Security+ 2-Month Study Plan (3/16 - 5/16)

1) Compliance & Governance (3/16 - 3/22)

- **Topics:** CIA Triad, Security Controls, Risk Management, Compliance Frameworks (NIST, ISO, GDPR, HIPAA), Legal & Ethical Issues
- **Practice:** 10-15 questions per day
- **Lab:** Review security policies & map controls to a framework

2) Vulnerabilities & Threats (3/23 - 4/5)

- **Topics:** Malware Types, Social Engineering, Network Attacks, Threat Intelligence, Vulnerability Management, Zero-Day Exploits
- **Practice:** 15-25 questions per day
- **Lab:** Analyze malware behavior in a sandbox

3) Security Operations (4/6 - 4/19)

- **Topics:** Firewalls, IDS/IPS, SIEM, Packet Capture, Endpoint Protection, Incident Response, Forensics, Logging, Disaster Recovery
- **Practice:** 20-30 questions per day
- **Lab:** Use Wireshark to analyze network traffic & investigate an event log file

4) Security Architecture (4/20 - 4/26)

- **Topics:** Secure Network Design, VPNs, Wireless Security, Segmentation, Zero Trust, Network Hardening
- **Practice:** 25-30 questions per day
- **Lab:** Configure a basic firewall rule

5) Security Implementation (4/27 - 5/10)

- **Topics:** IAM (Authentication Methods, MFA, Access Control Models), Cryptography (Encryption Types, Hashing, Digital Signatures, Certificates), Secure Protocols
- **Practice:** 30+ questions per day
- **Lab:** Set up MFA & generate/analyze a self-signed certificate

Final Review (5/11 - 5/16)

- **Practice:** Take 2 full-length practice exams
- **Review:** Focus on weak areas from practice exams
- **Lab:** Hands-on review of key security tools