CompTIA Security+ (SY0-701) Course Outline

Domain 1: Threats, Attacks, and Vulnerabilities

- 1.1 Malware Types and Functionality
  - Overview of different types of malware (viruses, worms, Trojans, ransomware)
  - Functions and behaviors of malware
- 1.2 Types of Attacks
  - Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
  - Man-in-the-Middle (MitM) attacks
  - Spoofing attacks and techniques
- 1.3 Social Engineering Attacks
  - Common social engineering techniques (phishing, pretexting, tailgating)
  - Countermeasures and prevention techniques
- 1.4 Application Attacks
  - SQL injection, cross-site scripting (XSS), buffer overflow
  - Mitigation techniques for application vulnerabilities
- 1.5 Mitigation and Deterrent Techniques
  - Security controls and countermeasures (firewalls, intrusion detection/prevention systems)
  - Security best practices and principles

Domain 2: Technologies and Tools

- 2.1 Network Component Installation and Configuration
  - Installation and configuration of routers, switches, and firewalls
  - VLAN configuration and management
- 2.2 Software Tools for Security
  - Network scanning tools (Nmap, Wireshark)
  - Vulnerability scanning tools
  - Log management and analysis tools
- 2.3 Hardware Tools for Security
  - Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
  - Physical security devices (biometric readers, CCTV)
- 2.4 Troubleshooting Common Security Issues
  - Identifying and resolving network security issues
  - Incident response procedures

Domain 3: Architecture and Design

- 3.1 Importance of Security Concepts in System Design
  - Secure network design principles
  - Defense-in-depth and layered security approaches
- 3.2 Security Implications of Embedded Systems
  - Security considerations for IoT devices

- Embedded system vulnerabilities and protections
- 3.3 Physical Security Controls
- Facility security measures (locks, alarms, access control)
- Environmental controls (HVAC, fire suppression)
- 3.4 Alternative Methods to Mitigate Security Risks
- Risk mitigation strategies (acceptance, avoidance, mitigation, transfer)
- Business continuity and disaster recovery planning

Domain 4: Identity and Access Management

- 4.1 Identity and Access Service Installation and Configuration
- Installation and configuration of identity services (LDAP, Active Directory)
- Authentication protocols (Kerberos, OAuth, SAML)
- 4.2 Implementation of Identity and Access Management Controls
- Role-based access control (RBAC)
- Multifactor authentication (MFA)
- 4.3 Common Account Management Practices
- User provisioning and de-provisioning
- Account policy enforcement and monitoring

Domain 5: Risk Management

- 5.1 Importance of Policies, Plans, and Procedures in Risk Management
- Security policies, standards, and procedures
- Security awareness and training programs
- 5.2 Concepts of Business Impact Analysis
- Identifying critical business functions and assets
- Assessing and mitigating business impact
- 5.3 Risk Management Processes and Concepts
- Risk assessment methodologies (qualitative vs. quantitative)
- Risk response strategies (mitigate, transfer, accept, avoid)

Domain 6: Cryptography and PKI (Public Key Infrastructure)

- 6.1 Basic Concepts of Cryptography
- Symmetric and asymmetric encryption algorithms
- Hashing algorithms and their uses
- 6.2 Use of Cryptography and PKI
- Digital signatures and certificates
- Public Key Infrastructure (PKI) components and services
- 6.3 Wireless Security Settings Configuration
- Securing wireless networks (WPA, WPA2, WPA3)
- Wireless encryption standards (WEP, WPA, WPA2)

Domain 7: Security Operations

- 7.1 Incident Response Procedures
  - Incident detection, response, and recovery
  - Forensic procedures and evidence collection
- 7.2 Disaster Recovery Plans Implementation
  - Business continuity planning (BCP) and disaster recovery planning (DRP)
  - Backup strategies and techniques
- 7.3 Comparison of Security Assessment Tools
  - Vulnerability assessment tools and techniques
  - Penetration testing methodologies (black-box, white-box, gray-box)

Domain 8: Network Security

- 8.1 Secure Network Architecture Concepts Implementation
  - Network segmentation and zoning
  - Virtual Private Networks (VPNs) and tunneling protocols
- 8.2 Security Concerns with Network Security Concepts
  - Network access control methods (802.1X, MAC filtering)
  - Security implications of IoT and BYOD environments
- 8.3 Security Concerns with Virtualization and Cloud Services
  - Virtualization security best practices
  - Cloud computing security considerations (shared responsibility model)

Domain 9: Compliance and Assurance

- 9.1 Policies, Plans, and Procedures related to Organizational Security
  - Legal and regulatory compliance requirements (GDPR, HIPAA, PCI DSS)
  - Security policies, standards, and guidelines
- 9.2 Risk Management Processes and Concepts
  - Risk assessment frameworks (NIST, ISO/IEC 27001)
  - Continuous monitoring and auditing practices