Accredited Institute of Information Technology
MAKING LEARNING ACCESSIBLE

CompTIA Security+ SYO-701

Security concepts, tools, and best-practice frameworks

A practical, student-friendly outline covering sY0-701 General Security Concepts, sY0-701 Threats, Vulnerabilities, and Mitigations, sY0-701 Secur...

MODULES	5
LESSONS	113
FORMAT	Self-paced

Module Breakdown

MODULE 1

SY0-701 General Security Concepts

1.0 Introduction to the Course
1.1 Fundamental Security Concepts
1.2 Zero Trust
1.3 Deception and Disruption
1.3.1 ACTIVITY - Testing a Honeypot
1.4 Security Controls
1.5 Change Management and Security
1.6 Cryptography Basics
1.6.1 ACTIVITY - Examining Symmetric Encryption
1.7 Asymmetric Encryption
1.7.1 ACTIVITY - Exploring Asymmetric Encryption
1.8 Hashing
1.8.1 ACTIVITY - Verifying Integrity with Hashing
1.9 Digital Certificates
1.10 Public Key Infrastructure
1.11 Data and Keys
1.12 Crypto Implementations
1.13 Blockchain

MODULE 1

SY0-701 General Security Concepts (continued)

1.14 Non-Cryptographic Data Protection

Module Breakdown (continued)

MODULE 2

SY0-701 Threats, Vulnerabilities, and Mitigations

2.1 Threat Actors and Motivations
2.2 Threat Vectors
2.2.1 ACTIVITY - O.MG Cable Baiting
2.2.2 O.MG-No Cable
2.3 Social Engineering
2.4 Operating System Vulnerabilities and Attacks
2.5 Application Vulnerabilities and Attacks
2.5.1 ACTIVITY - Performing a Buffer Overflow
2.6 Web-based Vulnerabilities and Attacks
2.6.1 ACTIVITY - Abusing Unsanitized Input
2.6.2 ACTIVITY - Grabbing Passwords with SQL Injection
2.6.3 ACTIVITY - Swiping a Token with XSS
2.7 Other Vulnerabilities
2.8 Common Malicious Activity Indicators
2.9 Insider Threat Indicators
2.10 Social Engineering Indicators

MODULE 2

SY0-701 Threats, Vulnerabilities, and Mitigations (continued)

2.10.1 ACTIVITY - Capturing Credentials through Social Engineering
2.11 Malware Activity Indicators
2.12 Operating System Attack Indicators
2.13 Application Attack Indicators
2.13.1 ACTIVITY - Recognizing Directory Traversal
2.14 Physical Attack Indicators
2.14.1 ACTIVITY - Quickly Cloning an RFID Badge
2.15 Network Attack Indicators
2.15.1 ACTIVITY - Crashing a Target with DoS
2.16 Cryptographic Attack Indicators
2.17 Password Attack Indicators
2.17.1 ACTIVITY - Password Cracking
2.18 Network Segmentation
2.19 Access Control
2.20 Enterprise Device Hardening

MODULE 3

SY0-701 Security Architecture

3.1 Network Segmentation
3.1.1 ACTIVITY - Segementing a Network
3.2 High Availability
3.3 Virtualization
3.3.1 ACTIVITY - Deploying Docker Containers
3.4 Cloud
3.5 Serverless Computing
3.6 IoT
3.7 ICS SCADA
3.7.1 ACTIVITY - Operating a SCADA System
3.8 RTOS and Embedded Systems
3.9 Reducing the Attack Surface
3.10 Firewalls
3.11 IDS IPS.mp4
3.12 Secure Communications - Access
3.13 Port Security
3.14 SD-WAN and SASE
3.15 Data Classifications

MODULE 3

SY0-701 Security Architecture (continued)

3.16 Protecting Data Types
3.17 Data Considerations
3.18 Redundancy
3.19 Alternate Sites
3.20 Multiple Platforms
3.21 Business Continuity

Module Breakdown (continued)

MODULE 4

SY0-701 Security Operations

4.1 Secure Baselines
4.2 Attack Surface Reduction
4.3 Wireless Installation
4.4 Wireless Security Settings
4.5 Mobile Solutions
4.5.1 ACTIVITY - Pwning a Mobile Device
4.6 Application Security Management
4.7 Asset Management
4.8 Vulnerability Management
4.9 Monitoring Activities
4.10 Monitoring Tools
4.10.1 ACTIVITY - Scanning a Network for Vulnerabilities
4.11 Firewall Configuration
4.11.1 ACTIVITY - Configuring Firewall Rules
4.12 Intrusion Detection Configuration
4.13 Web Traffic Filtering
4.14 Operating System Policy
4.14.1 ACTIVITY - Examining Windows Group Policy

MODULE 4

SY0-701 Security Operations (continued)

4.15 Network Service Security
4.16 Data Loss Protection
4.16.1 ACTIVITY - Checking File Integrity
4.17 Network Access Control
4.17.1 ACTIVITY - Require Multifactor Authentication
4.18 Identity Management
4.19 Access Management
4.19.1 ACTIVITY - Implementing Access Control
4.20 Security Automation
4.21 Incident Response
4.22 Digital Forensics

MODULE 5

SY0-701 Security Program Management and Oversight

5.1 Elements of Effective Security Governance
5.2 Elements of the Risk Management Process
5.3 Third Party Risk Assessment and Management
5.3.1 ACTIVITY - Analyzing the Solar Winds Supply Chain Failure
5.4 Effective Security Compliance
5.5 Audits and Assessments
5.5.1 ACTIVITY - Conducting OSINT
5.5.2 ACTIVITY - Performing Active Reconnaissance
5.6 Security Awareness Practices
5.7 Course Outro