CompTIA Advanced Security Practitioner (CASP) (Cas-003 R1.1)

Days: 5

Prerequisites: To be fit for this advanced course, you should have at least a foundational knowledge of information security.

Audience: This course is designed for IT professionals who want to acquire the technical knowledge and skills needed to conceptualize, engineer, integrate, and implement secure solutions across complex enterprise environments. The target student should aspire to apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security solutions that map to organizational strategies; translate business needs into security requirements; analyze risk impact; and respond to security incidents.

Description: 30 Bird's CompTIA Advanced Security Practitioner (CASP) CAS-003 course provides the knowledge needed to implement security solutions within an enterprise policy framework, using a vendor-neutral format. This includes risk and vulnerability management programs, organizational policies and training, applied cryptography, system security, network security, identity management, and incident response. This course maps to the CompTIA CASP certification exam. Objective coverage is marked throughout the course.

Students will benefit most from this course if you intend to take a CompTIA Advanced Security Practitioner CAS-003 exam.

OUTLINE:

CHAPTER 1: CYBERSECURITY FUNDAMENTALS

- Module A: Security concepts
- Module B: Risk management
- Module C: Threats and vulnerabilities

CHAPTER 2: RECOGNIZING VULNERABILITIES

- Module A: Common vulnerabilities
- Module B: Network vulnerabilities
- Module C: Application exploits

CHAPTER 3: VULNERABILITY MANAGEMENT

- Module A: Vulnerability Assessment
- Module B: Vulnerability management programs

CHAPTER 4: RECONNAISSANCE

- Module A: Reconnaissance techniques
- Module B: Active reconnaissance
- Module C: Analyzing scan results

CHAPTER 5: MONITORING NETWORKS

- Module A: Network security systems
- Module B: Logging and monitoring
- Module C: Network analysis

CHAPTER 6: POLICY DESIGN

- Module A: Security frameworks
- Module B: Security policies
- Module C: Controls and procedures

CHAPTER 7: SECURE NETWORK DESIGN

- Module A: Hardening networks
- Module B: Cryptography
- Module C: Hardening hosts and devices
- Module D: Secure application development

CHAPTER 8: IDENTITY MANAGEMENT

- Module A: Identity Systems
- Module B: Authentication technologies

CHAPTER 9: INCIDENT RESPONSE

- Module A: Incident response planning
- Module B: Incident response procedures
- Module C: Forensic toolkits