CompTIA Advanced Security Practitioner (CASP+)

Length: 5 Days

Prerequisites: To be fit for this advanced course, you should have at least a foundational knowledge of information security. This includes, but is not limited to:

- Knowledge of identity and access management (IAM) concepts and common implementations, such as authentication factors and directory services.
- Knowledge of cryptographic concepts and common implementations, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) and public key infrastructure (PKI).
- Knowledge of computer networking concepts and implementations, such as the TCP/IP model and configuration of routers and switches.
- Knowledge of common security technologies used to safeguard the enterprise, such as anti-malware solutions, firewalls, and VPNs.

Target Audience: This course is designed for IT professionals in the cybersecurity industry whose primary job responsibility is to secure complex enterprise environments. The target student should have real-world experience with the technical administration of these enterprise environments.

Summary: In this course, which prepares you for the CompTIA Advanced Security Practitioner exam (CAS-004),you will expand on your knowledge of information security to apply more advanced principles that will keep your organization safe from the many ways it can be threatened. You will 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; support IT governance and risk management; architect security for hosts, networks, and software; respond to security incidents; and more.

Course Objectives: In this course, you will analyze and apply advanced security concepts, principles, and implementations that contribute to enterprise-level security.

You will:

- Support IT governance in the enterprise with an emphasis on managing risk.
- Leverage collaboration tools and technology to support enterprise security.
- Use research and analysis to secure the enterprise.
- Integrate advanced authentication and authorization techniques.
- Implement cryptographic techniques, security controls for hosts and mobile devices, network security, and security in the systems and software development lifecycle.
- Integrate hosts, storage, networks, applications, virtual environments, and cloud technologies in a secure enterprise architecture.
- Conduct security assessments.
- Respond to and recover from security incidents.

COURSE CONTENT

Lesson 5: Performing Software Integration

Lesson 6: Explain Virtualization, Cloud and Emerging Technology

Lesson 7: Exploring Secure Configurations and System Hardening

Lesson 8: Understanding Security Considerations of Cloud and Specialized Platforms

Lesson 9: Implementing Cryptography

Lesson 10: Implementing Public Key Infrastructure (PKI)

Lesson 11: Understanding Threat and Vulnerability Management Activities

Lesson 12: Developing Incident Response Capabilities