

CompTIA Security+

Training &

Certification

© New Horizons, Pakistan, 2012

20F, 24th Commercial Street Phase 2 Ext. D.H.A. Karachi, Pakistan.

Tel: +9221-35317689-90, 35312084-85

Fax: +9221-35317696

Email us: info@nhpakistan.com

Website: www.nhpakistan.com.pk

Table of Contents

1.1	Objectives	3
1.2	Class Outline	4
1.3	Course Outline	5
1.4	Exam Outline	7

CompTIA Security+ Certification – Objectives

CompTIA Security+



CompTIA Security+ certification designates knowledgeable professionals in the field of security, one of the fastest-growing fields in IT.

CompTIA Security+ is an international, vendor-neutral certification that demonstrates competency in:

- Network security
- Compliance and operational security
- Threats and vulnerabilities
- Application, data and host security
- Access control and identity management
- Cryptography

CompTIA Security+ not only ensures that candidates will apply knowledge of security concepts, tools, and procedures to react to security incidents, it ensures that security personnel are anticipating security risks and guarding against them.

Candidate job roles include *security architect, security engineer, security consultant/specialist, information assurance technician, security administrator, systems administrator, and network administrator.*

Organizations that employ CompTIA Security+ certified staff include Hitachi Information Systems (Japan), Trendmicro (Philippines), Lockheed Martin, the U.S. State Department, Prestariang Systems Sdn. Bhd. (Malaysia) and U.S. government contractors such as EDS, General Dynamics and Northrop Grumman. CompTIA Security+ is one of the options for certifications required by the U.S. Department of Defense, for military personnel or military contractors engaged in information assurance activities.

The CompTIA Security+ certification is accredited by the [International Organization for Standardization \(ISO\)](#) and the [American National Standards Institute \(ANSI\)](#). The CompTIA Security+ certification may be kept current through the [CompTIA Continuing Education program](#).

CompTIA Security+ Certification - Class Outline

Duration:

Online Live - 5.00 Sessions

Online Anytime - Self Paced

Traditional Instructor Led Learning - 5.00 Day(s)

Mentored Learning - Flexible

Overview:

The CompTIA® Security+® (2011 Objectives) course is designed to help you prepare for the SY0-301 exam. Students will implement and monitor security on networks, applications, and operating systems, and respond to security breaches.

Who Should Attend:

This course is targeted toward an Information Technology (IT) professional who has networking and administrative skills in Windows-based TCP/IP networks and familiarity with other operating systems, such as OS X, Unix, or Linux, and who wants to further a career in IT by acquiring a foundational knowledge of security topics; prepare for the CompTIA Security+ Certification examination; or use Security+ as the foundation for advanced security certifications or career roles.

At Course Completion:

Upon successful completion of this course, students will be able to: - identify the fundamental concepts of computer security. - identify security threats and vulnerabilities. - examine network security. - manage application, data and host security. - identify access control and account management security measures. - manage certificates. - identify compliance and operational security measures. - manage risk. - manage security incidents. - develop business continuity and disaster recovery plans.

Prerequisite(s) or equivalent knowledge:

[CompTIA Network+ Certification \(Exam N10-005\)](#)

[CompTIA A+ Certification \(2009 Objectives\)](#)

Prerequisite Comments:

There are no enforced prerequisites, however the recommended prerequisites are the CompTIA Network+ certification and two years of technical networking experience with an emphasis on security.

CompTIA Security+ Certification – Course Outline

Outline:

Lesson 1: Security Fundamentals

- Information Security Cycle
- Information Security Controls
- Authentication Methods
- Cryptography Fundamentals
- Security Policy Fundamentals

Lesson 2: Security Threats and Vulnerabilities

- Social Engineering
- Physical Threats and Vulnerabilities
- Network-Based Threats
- Wireless Threats and Vulnerabilities
- Software Based Threats

Lesson 3: Network Security

- Network Devices and Technologies
- Network Design Elements and Components
- Implement Networking Protocols
- Apply Network Security Administration Principles
- Secure Wireless Traffic

Lesson 4: Managing Application, Data and Host Security

- Establish Device/Host Security
- Application Security
- Data Security
- Mobile Security

Lesson 5: Access Control, Authentication, and Account Management

- Access Control and Authentication Services
- Implement Account Management Security Controls

Lesson 6: Managing Certificates

- Install a Certificate Authority (CA) Hierarchy
- Enroll Certificates
- Secure Network Traffic by Using Certificates
- Renew Certificates
- Revoke Certificates
- Back Up and Restore Certificates and Private Keys
- Restore Certificates and Private Keys

Lesson 7: Compliance and Operational Security

- Physical Security

Legal Compliance
Security Awareness and Training

Lesson 8: Risk Management

Risk Analysis
Implement Vulnerability Assessment Tools and Techniques
Scan for Vulnerabilities
Mitigation and Deterrent Techniques

Lesson 9: Managing Security Incidents

Respond to Security Incidents
Recover from a Security Incident

Lesson 10: Business Continuity and Disaster Recovery Planning

Business Continuity
Plan for Disaster Recovery
Execute Disaster Recovery Plans and Procedures

CompTIA Security+ Certification – Exam Outline

Number of questions	100
Length of test	90 minutes
Passing score	750 (on a scale of 100-900)
Recommended experience	CompTIA Network+ certification and two years of technical networking experience, with an emphasis on security.
Languages	English, Korean <i>Coming soon:</i> German, Japanese
Exam codes	SY0-301, JK0-018