CompTIA Security+

SYLLABUS

This online seminar in CompTIA Security + leads students through the official CompTIA Security + Certification exam guide culminating in the CompTIA N+ certification exam. Students gain skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, and laws.

This seminar will be presented exclusively online as an on-demand course that students can complete at their own pace over a span of two months by accessing, reviewing, and completing a blend of video tutorials, labs and exercises. All the material needed to complete this seminar successfully is available online and made accessible to each enrolled student. Students will be provided a user ID and password to allow them access to view the material in the seminar. The user ID will also be used to track attendance, which is essential for successfully completing this seminar.

Books

- The Official CompTIA Security+ Student Guide (Exam SY0-501) 2019 Update eBook
- ISBN: 978-1-64274-236-7

Prerequisites

- **Basic computer literacy**:
  Students should be familiar with the use of personal computers. They will be expected to turn the devices on and off as necessary, and utilize human input devices like the keyboard and mouse to an adequate level of proficiency.

- **Familiarity with desktop operating systems:**
  Students will be required to be able to launch and close programs, navigate and manipulate the file system, and to browse the Internet to retrieve information and perform research.

- **CompTIA A+ Core 1 and 2, and CompTIA Network+ experience required.**

Instructor

Dwaine “Rob” Roberts

Dwaine “Rob” Roberts is a former Army Staff Sergeant who has been in Information Technology for over 12 years. He holds an MBA in Information Technology Management and over 10 industry certifications to include: CompTIA A+, Network+ and Security+.

Rob taught over 300 students while stationed at Fort Gordon as an Information Technology Instructor. During this time he ensured soldiers were DoD Manual 8570 Baseline Certification compliant by giving them the skills necessary to prepare for certification exams.

Rob received an honorable discharge in 2016, and he has continued educating students as the founder of IT Master Key, an Information Technology training company. He has taught over 10,000 students both virtually and in person.

Rob is also a veteran of the Global War on Terror and a service-connected, disabled veteran, with nearly eight years active in the US Army.

Credentialing

After completing this course, students will be prepared to take the CompTIA Security+ Exam SY0-501.

Courses

ITDT 104 - CompTIA Security+

In this class, students gain skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, and laws.

This course provides an analysis of computer networks and infrastructure basics. It also discusses the breakdown of network topologies according to logical and physical architectures and topological protocols.

Attacks, Threats and Vulnerabilities - Focusing on more threats, attacks, and vulnerabilities on the Internet from newer custom devices that must be mitigated, such as IoT and embedded devices, newer DDoS attacks, and social engineering attacks based on current events.

Architecture and Design - Includes coverage of enterprise environments and reliance on the cloud, which is growing quickly as organizations transition to hybrid networks.

Implementation - Expanded to focus on administering identity, access management, PKI, basic cryptography, wireless, and end-to-end security.

Operations and Incident Response - Covering organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls, and basic digital forensics.

Governance, Risk and Compliance - Expanded to support organizational risk management and compliance to regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.