MOORE NORMAN
TECHNOLOGY CENTER

Course Syllabus

Preparation for CompTIA Security+ Certification

CN350

Hours : In Class 54 Clinical Total 54

Description

Get the latest training for the 2019 update covering 100% of the objectives for Security+! You will learn how to handle threats, attacks, and vulnerabilities using industry-standard tools and technologies, while understanding the role of architecture and design. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your computer security skill set so that you can confidently perform your duties in any security-related role.
Tuition includes books and Test Prep for certification preparation, everything you need to enter the exam confident in your skill set.
Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.
While MNTC provides you with learning resources to prepare for a successful exam experience, certification exams must be scheduled through PearsonVUE. Exam may be taken in our Assessment Center. Certification Exam is not included. Student discounts are as much as 50%.

Prerequisites

CN221 CompTIA Network+ certification is highly recommended. If you have experience but are not sure how to assess your skill level, please call Rick Spaulding, program coordinator, at (405) 801-5704 to discuss your situation.

Books

CompTIA CertMaster Learn for Security+ (SY0-501)	- ISBN:	(Included)
CompTIA Labs for Security+ (SY0-501): 2019 Update	- ISBN:	(Included)
CompTIA Security+ SY0-501 Exam Cram (5th Edition)	- ISBN: 978-0789759009	(Suggested)

Learning Objectives

1. Compare and Contrast attacks
2. Compare and Contrast security controls.
3. Use security assessment tools.
4. Explain basic cryptography concepts.
5. Implement a public key infrastructure.
6. Implement identity and access management controls.
7. Manage access services and accounts.
8. Implement a secure network architecture.
9. Install and configure security appliances.
10. Install and configure wireless and physical access security
11. Deploy secure host, mobile, and embedded systems.
12. Implement secure network access protocols.
13. Implement secure network applications.
14. Explain risk management and disaster recovery concepts.
15. Describe secure application development concepts.
16. Explain organizational security concepts.

Teaching Philosophy

We believe that instructors, staff, and administrators have a shared responsibility to provide: 1) innovative course design and instruction; 2) a safe, learner-centered environment; and 3) an authentic learning experience.

Teaching Methods

Methods include lecture, class discussion and demonstrations.

Evaluation Methods

Student success is based on participation in class activities and the completion of exercises. A certificate of completion requires 100% attendance and completion of all assigned activities.

Grading Policy

Student success is based on participation in class activities and the completion of exercises. A certificate of completion requires successful completion of all assigned work within the established time frame. Types of graded assignments will be projects, review questions, activities, assignments and tests
Grading Policy:
A = 90 - 100%
B = 80 - 89%
C = 70 - 79%
D = 60 - 69%
F = Below 60%
A course grade of D does not qualify the course as a prerequisite to other courses.

Student Responsibilities

To ensure a quality and safe learning environment, students are required to follow the Post-Secondary Student Behavior policy #560. This policy can be found at www.mntc.edu/board-policies. Printed copies are available upon request.

Students are expected to attend class and participate in class discussions and activities, complete out of class assignments and exams in class.

Students must be on time and meet the attendance policy set for this class which is 80% attendance.