Compuserve Pvt Ltd.

Course Duration : 80 Hrs

CompTIA Network Security Professional

COURSE BROCHURE

www.cometcompuserve.com

A Career in Cybersecurity

With the increase in data breaches, information is vulnerable. Skilled IS professionals are in demand which means huge potential for job-seekers.

Get CompTIA certified and get to work.

Employment of information security analysts is projected to grow 28% from 2016 to 2026, much faster than the average for all occupations.

We at **COMET Compuserve** have partnered with **CompTIA** to prepare you for a career in the cybersecurity industry offering the most recognized entry-level certifications in the IT industry. CompTIA training covers breadth and depth across critical technology subject areas to help you advance your career in IT and prepare for CompTIA certifications.

Our Trainers will guide to to achieving the **CompTIA Network Security Professional** certification.

CompTIA Network Security Professional

Who will benefit from this training:

- Individual who are looking for a career change to cybersecurity
- Individuals who are looking for an entry level career in cybersecurity
- Students
- Security Analyst
- Security Operations Centre (SOC) Analyst
- Vulnerability Analyst
- Cybersecurity Specialist
- Threat Intelligence Analyst
- Security Engineer

What do you learn during this program?

You will achieve 3 certifications:

- CompTIA Security+
- CompTIA Cybersecurity Analyst (CySA+)
- CompTIA PenTest+

Duration:

The total duration for all the 3 courses is **80 hours**. If each course is taken individually the duration is 35 hours per course.

What do we provide:

Our trainers are **CompTIA Certified Instructors**. All participants will receive an official digital courseware and we will guide you to setting up the hands on labs on your laptops. The training will consists of 60% lectures and 40% labs.

Certification Exams

Certification exams are optional and this will have an additional cost. For participants to achieve the CompTIA Network Security Professional you will need to pass:

- CompTIA Security+
- CompTIA Cybersecurity Analyst (CySA+)
- CompTIA PenTest+

CompTIA Security+

Upon successful completion of this course, participants will learn to:

- Identify the fundamental concepts of computer security
- Identify security threats and vulnerabilities
- Manage data, application, and host security
- Implement network security
- Identify and implement access control and account management security measures
- Manage certificates
- Identify and implement compliance and operational security measures
- Manage risk
- Troubleshoot and manage security incidents
- Plan for business continuity and disaster recovery

Target Audience

This course is designed for information technology (IT) professionals who have networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks; familiarity with other operating systems, such as macOS®, Unix®, or Linux®; and who want to further a career in IT by acquiring foundational knowledge of security topics or using CompTIA Security+ as the foundation for advanced security certifications or career roles.

This course is also designed for participants who are seeking the CompTIA Security+ certification and who want to prepare for the **CompTIA Security+ SY0-601 Certification Exam.**

Prerequisites

A good working knowledge of Networking.

You can obtain this level of skills and knowledge by taking the CompTIA Network+ Certification course or by obtaining the appropriate industry certification.

CompTIA Cybersecurity Analyst (CySA+)

Upon successful completion of this course, participants will have learned to:

- Manage risks and vulnerabilities
- Configure and use threat detection tools
- Understand roles, responsibilities, and the security framework
- Perform data analysis and interpret the results to identify areas of concern
- Avoid, prevent, and respond to security incidents
- Contain and eradicate threats
- Understand security architecture, policies, and procedures
- Better secure and protect applications and systems

Target Audience

This course is designed primarily for cybersecurity practitioners who perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This course focuses on the knowledge, ability, and skills necessary to provide for the defense of those information systems in a cybersecurity context, including protection, detection, analysis, investigation, and response processes. In addition, the course ensures that all members of an IT team—everyone from help desk staff to the Chief Information Officer—understand their role in these security processes.

Prerequisites

CompTIA Security+ Certification (SY0-601)

CompTIA PenTest+

Upon successful completion of this course, participants will learn to plan, conduct, analyze, and report on penetration tests, including the ability to:

- Plan and scope penetration tests
- Conduct passive reconnaissance
- Perform non-technical tests to gather information
- Conductive active reconnaissance
- Analyze vulnerabilities
- Penetrate networks
- Exploit host-based vulnerabilities
- Test applications Complete post-exploit tasks
- Analyze and report pen test results

Target Audience

This course is designed for IT professionals who want to develop penetration testing skills to enable them to identify information-system vulnerabilities and effective remediation techniques for those vulnerabilities. Target students who also need to offer practical recommendations for action to properly protect information systems and their contents will derive those skills from this course.

This course is also designed for individuals who are preparing to take the CompTIA PenTest+ certification exam PT0-001, or who plan to use PenTest+ as the foundation for more advanced security certifications or career roles. Individuals seeking this certification should have three to four years of hands-on experience performing penetration tests, vulnerability assessments, and vulnerability management.

Prerequisites

To ensure your success in this course, you should have:

- Intermediate knowledge of information security concepts, including but not limited to identity and access management (IAM), cryptographic concepts and implementations, computer networking concepts and implementations, and common security technologies.
- Practical experience in securing various computing environments, including small to medium businesses, as well as enterprise environments.

You can obtain this level of skills and knowledge by taking the CompTIA Security+ Certification course or by obtaining the appropriate industry certification.

Our Students Testimonials

CONTACT US

Mobile : +91 9940068251 / 58251

Mail : ramesh@cometcompuserve.com / ilanchezhian@cometcompuserve.com