

ACI Learning

8200 IH-10 West Suite 1005

San Antonio, Texas 78230

Phone: (210)-277-4799

Toll Free: (866) 378-0761

Fax: (303) 768-0513

Catalog Number 1, Volume Number 6, Revised 12/15/2020

Effective Date 12/15/2020

Approved and Regulated by the Texas Workforce Commission, Career Schools and Colleges, Austin, Texas.

Table of Contents

[Introduction 3](#_Toc60061309)

[Administration Staff 3](#_Toc60061310)

[Faculty 4](#_Toc60061311)

[Programs Offered 4](#_Toc60061312)

[Tuition and Fees 6](#_Toc60061313)

[Class Schedule 6](#_Toc60061314)

[Full time Students: 7](#_Toc60061315)

[Part-Time Students: 7](#_Toc60061316)

[Entrance Requirements 7](#_Toc60061317)

[Enrollment 7](#_Toc60061318)

[Facilities 7](#_Toc60061319)

[Placement Assistance 10](#_Toc60061320)

[Attendance Requirements 10](#_Toc60061321)

[Certification Policy 11](#_Toc60061322)

[ACE Credit ASSESSMENT 12](#_Toc60061323)

[aci VIRTUAL LIVE offerings- HYBRID 13](#_Toc60061324)

[Grading System/Progress Reports 13](#_Toc60061325)

[Re-Admission Policy 13](#_Toc60061326)

[Graduation Policy 13](#_Toc60061327)

[Reschedule Policy 13](#_Toc60061328)

[Cancellation and Refund Policy 14](#_Toc60061329)

[Conduct Policy 16](#_Toc60061330)

[Student Complaints 16](#_Toc60061331)

[Educational Services 16](#_Toc60061332)

[Previous Credits 16](#_Toc60061333)

[Dismissal 16](#_Toc60061334)

[Student Grievance Procedure 16](#_Toc60061335)

[Programs 18](#_Toc60061336)

[Technical Support Specialist (TSS) 18](#_Toc60061337)

[Computer User Support Specialist (CUSS) 30](#_Toc60061338)

[Network Support Specialist (NSS) 48](#_Toc60061339)

[CCNA 62](#_Toc60061340)

[Information Security Analyst (ISA) 70](#_Toc60061341)

[Cybersecurity Specialist (CYBER) 82](#_Toc60061342)

[CompTIA security + 94](#_Toc60061343)

[IT Project Management Professional - CAPM/PMP 97](#_Toc60061344)

[CompTIA Network + 105](#_Toc60061345)

# Introduction

ACI Learning (hereinafter referred to as “The School”) offers job training programs that quickly close skill gaps and help individuals improve technical and management performance, producing rewarding careers and delivering an effective workforce for businesses across size and industry.

The School provides world-class technology and equipment for student training. The School is staffed with Instructors who must meet minimum certification standard in their field of specialty.

The School is an Authorized Training Partner for Microsoft, EC-Council, and CompTIA.

The School is approved by the State of Colorado Department of Education, Division of Private Occupational Schools (DPOS), Texas Veteran’s Commission, and by the Texas Workforce Commission (TWC).

The owner of the School is Chong Moua. ACI Learning is headquartered in Englewood, CO and as of this writing, offers classes on four campuses: Colorado Springs, Englewood, Jacksonville, San Antonio and Irving.

The School has the following history:

* January 2001: School is approved by the Colorado Board of Higher Education Department of Private Educational Schools under the name of Hensmann Training and Education Centers.
* February 2001: School opens its doors in Colorado Springs, CO and runs its first class.
* March 2001: School opens its second campus in Englewood, Colorado.
* July 2006: School is sold to new ownership. The acquiring company is LeaderQuest with one majority shareholder in George Cohlmia. School continues to operate as Hensmann Training and Education Centers through 2006 and into early 2007.
* April 2007: School officially changes its name from Hensmann Training and Education Centers to LeaderQuest.
* October 2014: School is approved by the Texas Workforce Commission
* October 2015: Purchased Consultech Inc. in Jacksonville, FL and is approved by Florida Department of Education.
* October 2016: Dallas approved for GI BILL ® Benefits
* June 2018: School opens fifth campus in San Antonio, Tx.
* May 2019: Acquired by MisTI Training Institute. Programs, policies and staff remain as-is.
* June 2020: School changes name from LeaderQuest to ACI Learning

# Administration Staff

Key Administrative Staff:

* Brett Shively- CEO
* Jerry Kukuchka – Chief Financial Officer
* Tim Kalil – Chief Operations Officer
* David Duke- Chief Product Officer
* Gary Van Prooyen- Chief Marketing Officer
* Bruce Stassen – Director of HR
* Jennifer Strobl – Director of Program Operations
* David Koker- Campus Director- San Antonio
* Bob Villareal – Campus Director – Irving
* Qwincy Houston – Campus Director – Denver
* Chris Young – Campus Director – Colorado Springs
* Jennifer Mathis – Campus Director – Jacksonville
* Meghan Jurado –Compliance Manager/Lead SCO
* Mary Walker – Accounting

San Antonio Staff:

* David Koker – Campus Director – San Antonio
* Angie Murica- Career Training Consultant
* Starla Condes- Career Training Consultant
* Michele Cruz- Career Training Consultant
* Karla Urbina- Employment Development Manager
* Sigourney Soughers- Frontline Associate
* William Wofford – Lead Technical Instructor

# Faculty

**William Wofford- Lead Technical Instructor**

William is an experienced instructor with hands-on experience in the real world. He works with the students using real world examples and ensures that they are completely immersed in the material for understanding and practice. He currently holds certifications in:

* CompTIA A+
* CompTIA Network +
* CompTIA Security +

# Programs Offered

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Program Title / Certificate** | **Course Number** | **Course Title** | **Contact Hours (Hrs)** | **Program Completion Length\* (Days)** |
| **Infrastructure and Tech Support** | | | | |
| Technical Support Specialist (TSS) | ITIL-FND | ITIL Foundations | 40 | 15 |
| 220-1001 | A+ Essentials | 40 |
| 220-1002 | A+ Practical Applications | 40 |
| Computer User Support Specialist (CUSS) | 220-1001 | A+ Essentials | 40 | 25 |
| 220-1002 | A+ Practical Applications | 40 |
| N10-007 | Network+ | 40 |
| SY0-601 | Security+ | 40 |
| ITIL-FND | ITIL Foundations | 40 |
| CCNA | CCNA 1 | Certified Cisco Network Administrator, CCNA Part 1 | 40 | 10 |
| CCNA 2 | Certified Cisco Network Administrator, CCNA Part 2 | 40 |
| Network Support Specialist (NSS) | N10-007 | Network+ | 40 | 20 |
| SY0-601 | Security+ | 40 |
| CCNA 1 | Certified Cisco Network Administrator, CCNA Part 1 | 40 |
| CCNA 2 | Certified Cisco Network Administrator, CCNA Part 2 | 40 |
| CompTIA Network + (Net +) | N10-007 | Comp Network + | 40 | 5 |
| AWS re-Start Cloud Support | AWS | AWS Fundamentals, Cloud & SysOps | 320 | 40 |
| **Information Security** | | | | |
| Information Security Analyst- ISA | SY0-601 | Security + | 40 | 15 |
| CND | Certified Network Defender | 40 |
| CEH | Certified Ethical Hacker | 40 |
| Cybersecurity Specialist (CYBER) | SY0-601 | Security+ | 40 | 15 |
| CEH | Professional Ethical Hacker | 40 |
| CHFI | Computer Hacking Forensics Investigator | 40 |
| CompTIA Security + | SY0-601 | Security + | 40 | 5 |
| **Project and Service Management** | | | | |
| IT Project Management Professional | ITIL | ITIL Foundations | 40 | 10 |
| CAPM/PMP | PMP Exam Preparation | 40 |

\*Program Completion Length does not include self-study test prep time based on industry standard of 1 day of self-study test prep for each day of course lecture.

# Tuition and Fees

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Programs** | | | | | | | | |
| **Tuition** | **Labs** | | | | | **Total Tuition Fee** | | |
| Technical Support Specialist (TSS) – 120 hours | | | | | | | | |
| $7,818 | | | $267 | | $8,085 | | | |
|  | | | | | | | | |
| AWS re/Start Cloud Support (AWS)- 320 hours | | | | | | | | |
| $13,875 | Included | | | | $13,875 | | | |
| Computer User Support Specialist (CUSS) – 200 hours | | | | | | | | |
| $13,342 | $533 | | | | | $13,875 | | |
|  | | | | | | | | |
| Cisco Certified Network Associate (CCNA) – 80 hours | | | | | | | | |
| $6,192 | $398 | | | | | $6,590 | | |
|  | | | | | | | | |
| Network Support Specialist (NSS) – 160 hours | | | | | | | | |
| $11,618 | $762 | | | | | $12,380 | | |
|  | | | | | | | | |
| IT Project Management Professional – 80 hours | | | | | | | | |
| $5,399 | $191 | | | | | $5,590 | | |
|  | | | | | | | | |
| Information Security Analyst- (ISA)- 120 Hours | | | | | | | | |
| $9,432 | $1,053 | | | | | $10,485 | | |
|  | | | | | | | | |
| Cybersecurity Specialist (CYBER) – 120 hours | | | | | | | | |
| $9,160 | $1,325 | | | | | $10,485 | | |
|  | | | | | | | | |
| CompTIA Security + (SY0-501) – 40 hours | | | | | | | | |
| $2,713 | | | | $182 | | | | $2,895 |
|  | | | | | | | | |
| CompTIA Network+ (N10-007) – 40 hours | | | | | | | | |
| $2,713 | | $182 | | | | | $2,895 | |

# Class Schedule

All courses are determined by Vendor standards. Not all programs have been submitted for GI Bill ® benefits. Please see our website at: [http://www.ACI Learningonline.com](http://www.leaderquestonline.com/it-career-training/) for our current class schedule as we offer classes as the need arises to better serve our students.

## Full time Students:

Monday through Friday 8:00am – 5:00 pm with one-hour lunch break, mornings 8:00am to 12:00 pm or afternoons from 1:00pm to 5:00pm. All full-time students attend 20 hours a week or more.

## Part-Time Students:

Monday through Friday 7:00pm – 11:00pm.

When an unexpected closure occurs due to extraordinary conditions such as inclement weather, students will be notified as soon as possible by phone and/or radio, and/or TV who provide closure information as a public service. Classes are not held on the following holidays:

New Year’s Eve Labor Day

New Year’s Day Thanksgiving Day & the Friday following

Memorial Day Christmas Eve

Independence Day Christmas Day

# Entrance Requirements

The school does not discriminate based on race, sex, religion, ethnic origin, or disability.

Prospective students must have a high school diploma or equivalency diploma with the willingness to learn; and a working knowledge of computers would be greatly appreciated. We also screen our students to make sure they will be successful with our program. In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

# Enrollment

Prospective students may enroll anytime. Late enrollments will be only one week prior to class start time and as late as one day into first class, depending on the program and the student has adequate experience.

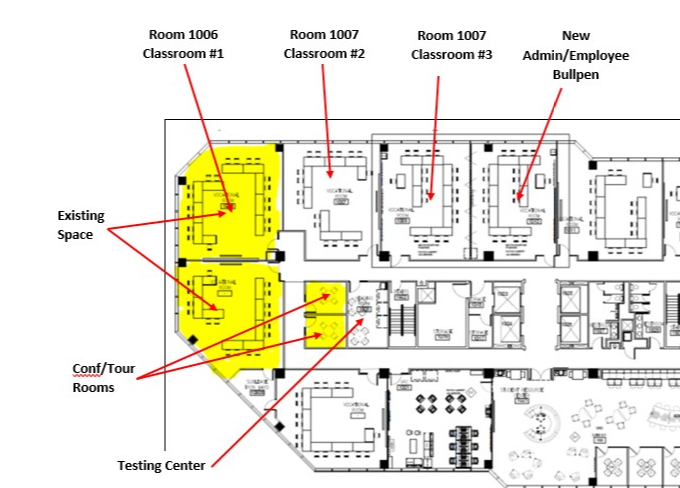
# Facilities

The ACI Learning main corporate office is located in Denver at 6855 S. Havana St STE 200, Centennial CO 80112. ACI Learning has a campus in Dallas, TX at 102 Decker Court, Ste 250, Irving, TX 75062. ACI Learning also operates a training facility in Colorado Springs at 7450 Campus Dr, Ste 250, Colorado Springs, CO 80920 and a facility at 8663 BayPines Rd Bldg 4 Suite 104, Jacksonville FL 32256. The newest facility is located in San Antonio at 8200 IH-10 West Suite 1005, 78230. Hours of operation are from 8 am to 11 pm. All classrooms are furnished with the latest state-of-the-art equipment and furniture. A Resource Center, Study Center and Career Services Center are available to students.

ACI Learning is a smoke-free environment. For those that smoke, designated smoking areas are located outside our training facilities.

Below is a full accounting of each of the school’s facilities as of April 15, 2020:

|  |  |  |  |
| --- | --- | --- | --- |
| **Englewood, CO** | | | |
|  | Address | | 6855 S Havana St, Suite 230, Centennial, CO 80112 |
|  | Total Square Footage | | 6,932 Sq. Ft. |
|  | Number of Classrooms | | 3 |
|  | Student Stations in Classroom #1 | | 16 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #2 | | 18 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #3 | | 18 Dell Optiplex machines with dual monitors |
|  | Lab Environment | | A separate lab environment integrated into each classroom |
|  | Virtual Live Training Room Description | | 3 workstations dedicated to virtual live training. |
|  | Student Self Study and Test Prep Room Description | | 3 workstations dedicated to self-study or test preparation. |
|  | Administrative Area Description | | 10 Cubicles  8 Enclosed Offices  2 Conference Rooms  1 Break Area  1 Reception Area |
| **Colorado Springs, CO** | | | |
|  | Address | | 7450 Campus Drive, Suite 250 Colorado Springs, CO 80920 |
|  | Total Square Footage | | 5,049 Sq. Ft. |
|  | Number of Classrooms | | 4 Classrooms |
|  | Student Stations in Classroom #1 | | 20 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #2 | | 20 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #3 | | 18 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #4 | | 24 Dell Optiplex machines with dual monitors |
|  | Virtual Live Training Room Description | | 2 workstations dedicated to virtual live training. |
|  | Student Self Study and Test Prep Room Description | | 2 workstations dedicated to self-study or test preparation. |
|  | Administrative Area Description | | 2 Enclosed Offices  4 Conference Rooms  1 Employee Bullpen Area  1 Break Area  1 Reception Area  1 Testing Area |
| **Jacksonville, FL** | | | |
|  | Address | 8663 Baypine Rd Building 4, Suite 104 Jacksonville, FL 32256 | |
|  | Total Square Footage | 5,959 Sq. Ft. | |
|  | Number of Classrooms | 3 Classrooms | |
|  | Student Stations in Classroom #1 | 16 Dell Optiplex machines with dual monitors | |
|  | Student Stations in Classroom #2 | 16 HP Pro 3500 machines with dual monitors | |
|  | Student Stations in Classroom #3 | 12 Dell Optiplex machines with dual monitors | |
|  | Pearson Vue Testing Center | 3 HP Prodesk 405 workstations dedicated to Testing | |
|  | Administrative Area Description | 3 Enclosed Meeting Offices  1 Conference Area  1 Break Area  1 Reception Area  Open office space with 8 cubicles  1 Enclosed Director’s office. | |
|  |  | |  |
| **Irving, TX** | | | |
|  | Address | | 102 Decker Court, Suite No. 250 Irving, TX 75062 |
|  | Total Square Footage | | 4,977 Sq. Ft. |
|  | Number of Classrooms | | 3 Classrooms |
|  | Student Stations in Classroom #1 | | 16 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #2 | | 16 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #3 | | 18 Dell Optiplex machines with dual monitors w/ a hands on lab environment |
|  | Testing Center | | PearsonVue Testing Center |
|  | Administrative Area Description | | 3 Enclosed Offices  1 Conference Room  1 Break Area  1 Reception Area  1 Employee Bullpen Area |
| **San Antonio, TX** | | | |
|  | Address | | 8200 IH-10 West, Suite 1005, San Antonio, TX 78230 |
|  | Total Square Footage | | 4,350 Sq. Ft. |
|  | Number of Classrooms | | 3 Classrooms |
|  | Student Stations in Classroom #1 | | 16 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom # 2 | | 16 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #3 | | 16 Dell Optiplex machines with dual monitors |
|  | Administrative Area Description | | 1 Office  1 Conference Room  1 Break Area  1 Reception Area  1 Employee Bullpen Area |
| **Facility includes highlighted area below.** | | | |



# Placement Assistance

ACI Learning offers job lead referrals as they are sent to us from employers. However, we make no guarantee, express or imply of future employment. Current law prohibits any school from guaranteeing job placement as an inducement to enroll students.

# Attendance Requirements

Students are expected to arrive on time for classes with the proper materials and attitude. An overall attendance rate of at least 80% is required. Instructors take attendance on a daily basis through an attendance log that is submitted to student services by 11:00AM each day and added to the student’s file. On that attendance log, instructors mark whether the student was tardy, absent, or partial. Instructors may request students to withdraw from a course or program if excessive absences of over 75% or tardiness lead to unsatisfactory progress.

Students who fall behind the 80% attendance rate or the 80% lab participation rate will be put on academic probation by student services and if they fall under 75% will automatically be dropped from the program. If students using VA benefits exceeds 75% total absences per period will be terminated from their VA benefits for unsatisfactory attendance. All students will be given one additional training period after they are put on probation to meet requirement or will be terminated at that time.

ACI Learning will not terminate the enrollment of a student for lack of attendance at a point at which a refund would not be due (75%). We will charge for a full day of absence if the student fails to attend all of the scheduled classes on a scheduled class day and will charge for a partial day of absence for any period of absence during the day. We measure class in two hour increments, any attendance over six hours is considered a full day and any attendance under two hours will be considered an absence.

ACI Learning does not consider school holidays, such as summer vacation and Christmas holidays, etc., as days of absence.

In order to show that the cause of unsatisfactory attendance has been removed, students must show good attendance (as defined) for one period after being terminated for unsatisfactory attendance.  After such time, the student may be recertified for VA education benefits.

Students who are unable to continue classes for medical reasons or severe personal problems will be required to take a leave of absence until that are able to return to class. Proper documentation will be required to substantiate a student’s withdrawal. We also offer an audit policy. Students can come and refresh any class on a space availability basis.

In a 12-month calendar period, a student may have no more than two leaves of absence. For a program with course time of 200 hours or less, a student may be on leave of absence for a total of 30 calendar days with proper notification and planning with their Learning Consultant.

A student who is obligated for the full tuition may request a grade of “incomplete” if the student withdraws for an appropriate reason unrelated to the student’s academic status. A student who receives a grade of incomplete may re-enroll in the program during the 12-month period following the date the student withdraws and complete those incomplete subjects without payment or additional tuition for that portion of the course or program.

Certification Policy

As part of our commitment to student success, unless otherwise noted, ACI Learning covers the cost of one certification attempt per class for students that meet the preparation guidelines. Upon completion of study time, one certification attempt per completed class outlined on the registration paperwork will be covered to enable the student to complete their education. Students are eligible to schedule a certification attempt appointment after completing each class in their program. The following policy statements outline conditions and requirements associated with certification:

It is highly recommended that any certification prep, labs, study guides and materials included in the program are completed before attempting certification. It is the Student’s responsibility, and to their advantage, to utilize resources both included in the program and outside of the program to ensure their readiness. For every hour of class time, we expect a student to study an additional 2 to 3 hours on their own to be able to pass the vendor certification.

Students are encouraged to take all certifications at the ACI Learning facility on campus. Students must complete 80% of class before they can request their certification appointment be covered by contacting: [clientservices@acilearning.com](mailto:clientservices@acilearning.com) .

Students are limited to only one attempt per class. In the event a student fails an attempt, they will have three options:

1. Exchange one of the other course attempts included in a program
2. Pay out of pocket
3. Elect not to retake and move on to the other courses in the program

Once registered at our center, ACI Learning requires a minimum of 48 hours in advance for reschedule or the appointment may be void. Missed appointments cannot be recovered and eligibility to take that attempt will be lost.

Certification attempts are required to be taken within 6 months from the last day of a completed class at the campus facility in order to complete training. Requests for certification attempts outside of this window are granted at ACI Learning’s discretion.

ACE Credit ASSESSMENT

ACE credits are an optional way for students to link their studies into credits that may be transferable to other schools and colleges. These credits are not required in order to complete the training program and are not part of tuition and fees. Any student wishing to participate in ACE credits does so voluntarily and covers the cost of all credits.

In order to be granted ACE credits for qualifying classes, a student must take and achieve a 70% or higher score on the class assessment. The assessment links objectives and learning outcomes covered during the course. It is designed to evaluate the knowledge and skills the student has obtained by the completion of class, and was created by experienced faculty who hold credentials associated with the subject matter. If the student does not score a least 70%, a retake assessment can be attempted. The retake assessment score is considered final and no additional retakes will be offered. Students re-sitting classes will not be eligible to take the assessment.

In order to qualify to sit for the assessment, students must:

* Meet the required 80% participation/attendance by the last day of class.
* Students who elect to earn ACE credit hours for the course will need to score a minimum of 70% on the assessment.
* If student does not elect to earn ACE credit for the course, the score will be recorded but will not affect student status.
* If the student does not attend and complete the assessment on the last day of class due to a documented unforeseen circumstance outside of their control (emergency, medical, weather), permission may be granted to reschedule the assessment if the student contacts [Client](mailto:ClientServices@LeaderQuest.net) Services within 24 hours of their absence.
* If the student does not attend and complete the assessment on the last day of class, with no documented unforeseen circumstance outside of their control (emergency, medical, weather) or with no communication to ACI Learning, the student may not receive participation for the last day of class, nor receive ACE credits and may need to retake the class to earn completion and be granted another opportunity to take the assessment.

# aci VIRTUAL LIVE offerings- HYBRID

ACI Learning offers the opportunity to attend our classes in a hybrid synchronous learning session. Students will be taught in real-time, with their questions addressed by an instructor over audio and in chat. Students will participate in guided labs operated on state-of-the-art virtual servers and are guided through each exercise using the latest online texts. Students can attend in person on campus, or with the ability to log-in online and complete the course offsite if approved to do so.

ACI Learning records all virtual classroom sessions for internal audit and compliance purposes. By logging into your course you are consenting to being recorded.  Recorded Class content will not be distributed to any outside entity

# Grading System/Progress Reports

Our grading system is pass/fail as required by vendor certification. Student must be present in 80% of classes and must participate in 80% of course labs or else they will be put on academic probation. If the student falls below the 75% attendance and/or lab completion the student will be evaluated on course content and asked to re-sit the course at a later date if needed. All students will be given one additional training period after they are put on probation to meet requirements or will be terminated at that time. For programs 40 hours and under, there will be no probationary periods. For programs 80 hours and above, a probationary period of 40 hours will be implemented.

Students receive certificates of completion at the end of each course if the above requirements are met. All students have the option of refreshing classes for the lifetime of the course while it is being offered at no additional cost. Students may have a Progress report completed by their Instructor at the end of every course upon request.

# Re-Admission Policy

The school may allow a student whose enrollment was terminated for unsatisfactory progress to reenroll after a minimum of one probationary progress evaluation period. For programs 40 hours and under, there will be no probationary periods. For programs 80 hours and above, a probationary period of 40 hours will be implemented.

Such reenrollment does not circumvent the approved refund policy.

# Graduation Policy

To graduate and receive a Certificate of Completion, students must be present in 80% of classes and must participate and successfully complete 80% of course labs.

# Reschedule Policy

ACI Learning is committed to keeping class sizes small in order to facilitate a high quality learning environment for our Students.  Many classes are full at 14-18 Students; because of this we have to minimize reschedules as much as possible Taking into account any unforeseen circumstances that may occur, ACI Learning’s Reschedule Policy allows any student to reschedule their classes within their Program a maximum amount of 2 times total with no penalty or charge.  Beyond two reschedules, ACI Learning Students will be dropped from their program and provided a refund for the remaining classes per the cancellation policy below.

# Cancellation and Refund Policy

A full refund will be made to any student who cancels the enrollment contract within 72 hours (until midnight of the third day excluding Saturdays, Sundays and legal holidays) after the enrollment contract is signed or within the student’s first three scheduled class days.

1. Refund computations will be based on scheduled course time of class attendance through the last date of attendance. Leaves of absence, suspensions and school holidays will not be counted as part of the scheduled class attendance.

2. The effective date of termination for refund purposes will be the earliest of the following:

(a) The last day of attendance, if the student is terminated by the school;

(b) The date of receipt of written notice from the student; or

(c) Ten school days following the last date of attendance.

3. If tuition and fees are collected in advance of entrance, and if after expiration of the 72-hour cancellation privilege the student does not enter school, not more than$100 in nonrefundable administrative feesshall be retained by the school for the entire residence program or synchronous distance education course*.*

4. If a student enters a residence or synchronous distance education program and withdraws or is otherwise terminated, the school or college may retain not more than $100 in nonrefundable administrative fees for the entire program. The minimum refund of the remaining tuition and fees will be the pro rata portion of tuition, fees, and other charges that the number of hours remaining in the portion of the course or program for which the student has been charged after the effective date of termination bears to the total number of hours in the portion of the course or program for which the student has been charged, except that a student may not collect a refund if the student has completed 75 percent or more of the total number of hours in the portion of the program for which the student has been charged on the effective date of termination.[[1]](#footnote-1)

5. Refunds for items of extra expense to the student, such as books, tools, or other supplies should be handled separately from refund of tuition and other academic fees. The student will not be required to purchase instructional supplies, books and tools until such time as these materials are required. Once these materials are purchased, no refund will be made. For full refunds, the school can withhold costs for these types of items from the refund as long as they were necessary for the portion of the program attended and separately stated in the enrollment agreement. Any such items not required for the portion of the program attended must be included in the refund.

6. A student who withdraws for a reason unrelated to the student’s academic status after the 75 percent completion mark and requests a grade at the time of withdrawal shall be given a grade of “incomplete” and permitted to re-enroll in the course or program during the 12-month period following the date the student withdrew without payment of additional tuition for that portion of the course or program.

7. A full refund of all tuition and fees is due and refundable in each of the following cases:

1. An enrollee is not accepted by the school;
2. If the course of instruction is discontinued by the school and this prevents the student from completing the course; or
3. If the student's enrollment was procured as a result of any misrepresentation in advertising, promotional materials of the school, or representations by the owner or representatives of the school.

*A full or partial refund may also be due in other circumstances of program deficiencies or violations of requirements for career schools and colleges.*

8. REFUND POLICY FOR STUDENTS CALLED TO ACTIVE MILITARY SERVICE.

A student of the school or college who withdraws from the school or college as a result of the student being called to active duty in a military service of the United States or the Texas National Guard may elect one of the following options for each program in which the student is enrolled:

(a) if tuition and fees are collected in advance of the withdrawal, a pro rata refund of any tuition, fees, or other charges paid by the student for the program and a cancellation of any unpaid tuition, fees, or other charges owed by the student for the portion of the program the student does not complete following withdrawal;

(b) a grade of incomplete with the designation "withdrawn-military" for the courses in the program, other than courses for which the student has previously received a grade on the student's transcript, and the right to re-enroll in the program, or a substantially equivalent program if that program is no longer available, not later than the first anniversary of the date the student is discharged from active military duty without payment of additional tuition, fees, or other charges for the program other than any previously unpaid balance of the original tuition, fees, and charges for books for the program; or

(c) the assignment of an appropriate final grade or credit for the courses in the program, but only if the instructor or instructors of the program determine that the student has:

(1) satisfactorily completed at least 90 percent of the required coursework for the program; and

(2) demonstrated sufficient mastery of the program material to receive credit for completing the program.

9. The payment of refunds will be totally completed such that the refund instrument has been negotiated or credited into the proper account(s), within 60 days after the effective date of termination.

# Conduct Policy

Students are expected to act in an adult manner. Possessions of weapons, illegal drugs, and alcohol of any kind are not allowed at any time. The school does not tolerate sexual harassment. Any violation of school policies may result in permanent dismissal from school.

# Student Complaints

Student complaints will be brought to the attention of the School in order to be resolved by emailing [david.koker@acilearning.com](mailto:david.koker@acilearning.com) . If the student complaint cannot be resolved between the student and the school, a student may contact the State authorizing body for the school – typically that would be the Division of Private Occupational Schools. In Texas, complaints can be mailed to:

TWC-Career Schools and Colleges

101 East 15th Street, Room 226T

Austin, Texas, 78778-0001

faxed to (512) 936-3111; or emailed [www.texasworkforce.org/careerschoolstudents](http://www.texasworkforce.org/careerschoolstudents). All student complaints must be submitted to the school and Division in writing. There is a two-year limitation on Division action on student complaints.

# Educational Services

ACI Learning’s primary educational format is traditional classroom instruction with online content as an adjunct learning resource. When the student’s schedule or personal circumstance prevents them from participating physically, ACI Learning does provide instructor led online training as an alternate method of training. Each ACI Learning training facility offers students a break room and a study area for their convenience.

# Previous Credits

Credit for previous education will be evaluated and when appropriate, credit will be granted and the program shortened accordingly. ACI Learning does not guarantee the transferability of its credits to any other institution unless there is written agreement with another institution.

# Dismissal

Any student may be dismissed for violations of rules and regulations of the school, as set forth in the school’s publications. A student also may be withdrawn from classes if he or she does not prepare sufficiently, neglects assignments, or makes unsatisfactory progress. The director, after consultation with all parties involved, makes the final decision.

# Student Grievance Procedure

Students can bring any grievance to the attention of the school in order for the school to help resolve any issues that may occur. Grievances should be sent via email to the Campus Director at [dkoke](mailto:dkoke)r@acilearning.com. Any grievances unresolved by the school should be sent to:

Texas Workforce Commission  
Career Schools and Colleges  
101 E. 15th Street  
Austin, TX 78778-0001

APPROVED AND REGULATED BY THE TEXAS WORKFORCE COMMISSION, CAREER SCHOOLS AND COLLEGES, AUSTIN, TEXAS.

# Programs

## Technical Support Specialist (TSS)

Program Description

This program is designed to quickly help individuals get to work in entry level jobs in the field of IT as Technical Support Specialists. This program develops the skills required to perform the following job functions:

* Install, build, maintain, and configure personal computers, laptop computers, and printers
* Principles of physical and TCP/IP networks, as well as the operational and professional procedures as an IT technician
* Support personal computers, mobile devices, and small networks in a business setting
* Troubleshoot hardware and software
* Install and configure Windows and other Operating Systems
* Examine server hardware and software, disaster recovery strategies
* Perform installation, troubleshooting, and management functions in the Windows Client operating system environment.
* The program also introduces the principles and core elements of IT service management (ITSM) based on ITIL framework

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| ITIL | ITIL Foundations | 20/20/0/40 |
| 220-1001 | CompTIA A+ Essentials | 20/20/0/40 |
| 220-1002 | CompTIA A+ Practical Applications | 20/20/0/40 |

The approximate time required to complete this program is three weeks for day students and six weeks for evening students.

### Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00 PM for 25 days. Classes for evening students will be held on Monday through Friday 7:00 to 11:00pm. For day students, an hour lunch break will be taken every day from 11:30AM to 12:30PM with four 10 minutes breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

Tuition and Fees

Registration: $0  
Tuition: $7,818  
Labs: $267  
Total Tuition Fee: $8,085

Targeted Job Roles

* Technical Support Specialist
* Helpdesk Technician
* Computer Technician
* IT Support Specialist

Subject Descriptions and Syllabi

#### ITIL foundations

course DESCRIPTION

Based on the ITIL best practice service lifecycle methodology, this subject provides a practical understanding of the key concepts, principles, processes, and functions that enable successful IT Service Management (ITSM) provisioning. The course intent is to provide proven practical guidance on how to successfully introduce an integrated IT Service Management framework and how best practices can be adopted and adapted within an organization. It also prepares students for the ITIL Foundation Certificate. This is for IT practitioners involved in the strategy, design, implementation and on-going delivery of business-used IT services and for anyone who requires an insight into Service Management best practices.

course OBJECTIVES

Upon completion of the ITIL Foundations training, participants will understand:

* Key concepts of ITIL
* Important principles for improving IT operations and project success
* Vital processes and functions
* Practical guidance for applying ITIL to everyday IT project situations
* How to align with business, control costs, and improve IT service quality
* Strategies to balance IT resources

Targeted Job Roles

* IT Professionals with an interest in Service Management

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills

Class Schedule

Day students will attend weekday classes from 8:00AM to 5:00PM for five days. Classes for evening students will be held Monday through Friday from 7:00 PM to 11:00 PM. For day students, an hour lunch break will be taken every day from 11:30AM to 12:30PM with four 10 minute breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| ITL-FND | ITIL Foundations | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

ITIL 4 Foundation

Course Developer: Logical Operations

Authors: Patrick Von Schlag ITIL Expert

Laurie Perry

Publish Date2019

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

**Day 1**

Module 1: Introduction

* Introduction/Housekeeping
* Introduction to key ITIL concepts
* IT as a Service
* Introduction to processes and process management
* The Service Lifecycle approach

Module 2: Service Strategy

* Purpose, goal, objectives & Scope
* Value Creation through Services
* Assets - Resources and Capabilities
* Service Strategy - Main activities
* Service Strategy processes
* Service Portfolio management
* Demand management
* Financial management
* Business Relationship Management

**Day 2**

Module 3: Service Design

* Purpose, goal, objectives & Scope
* Service Design processes
* The 4 P's
* Service Design aspects
* Service Catalog Management
* Service Level Management
* Capacity Management
* Availability Management
* IT Service Continuity Management
* Service Portfolio
* Information Security Management
* Supplier management
* Design Coordination

Module 4: Service Transition

* Purpose, goal, objectives & Scope
* Service Transition value to the business
* Technology and architecture in Service Transition
* Service Transition Processes
* Change Management
* The 7 R's of Change Management
* Service Asset and Configuration Management
* Release and Deployment Management
* Knowledge Management

**Day 3**

Module 5: Service Operation

* Purpose, goal, objectives & Scope
* Service Operation definitions
* The Service Desk
* Technical Management
* Application Management
* IT Operations Management
* Service Operations Processes
* Event Management
* Request Fulfillment
* Problem Management
* Access Management

Review Session

**Day 4**

Module 6: Continual Service Improvement

* Purpose, goal, objectives & Scope
* Models and Processes
* The Deming Cycle
* Measurement and metrics
* Continual Service Improvement activities
* Risk management
* Continual Service Improvement interfaces
* Interface with Service Level Management
* Review Session

**Day 5**

* Review Session
* Certification Attempt

Grading

Grading will be assigned as follows:

* Attendance: 75%
* Exercise Participation: 25%

CompTIA A+ 1001 Essentials

This course will build on the student's existing user-level knowledge and experience with personal computer (PC) hardware to present fundamental skills and concepts that are used on the job. In this course, the student will acquire the essential skills and information needed to install, configure, troubleshoot, upgrade, and perform preventive maintenance on PCs and mobile device hardware.

The CompTIA A+ course can benefit the student in two ways. Whether working in a   
mobile or corporate environment with a high level of face-to-face customer interaction, where client   
communication and client training are important, or in an environment with limited customer   
interaction and an emphasis on hardware activities, this course provides the background knowledge and skills required to be a successful A+ technician.

In this course, the student will install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers, digital devices, and operating systems.

COURSE OBJECTIVES

* Install and configure PC system unit components and peripheral devices.
* Install, configure, and troubleshoot display and multimedia devices.
* Install, configure, and troubleshoot storage devices.
* Install, configure, and troubleshoot internal system components.
* Explain network infrastructure concepts.
* Configure and troubleshoot network connections.
* Implement client virtualization and cloud computing.
* Support and troubleshoot laptops.
* Support and troubleshoot mobile devices.
* Install, configure, and troubleshoot print devices.

Course hours

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Contact Hours** |
| A+ 1001 | CompTIA A+ Essentials | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for night students.

REQUIRED COURSEWARE

* CompTIA A+ Certification, Exam 220-1001 (ebook from CompTIA)
* ACI Learning Learning Management System Student Portal
* TestOut Test Prep
* Professor Messer Guides
* TestOut Labs and ACI Learning Labs

iNSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs (virtual)
* Hand on in-class PC build
* Videos
* Assessments

COURSE Outline

**Day 1**

**Introductions/Policy Overview/Course Description**

**Lesson 1: Installing and Configuring PC Components**

Topic A: Use Appropriate Safety Procedures

Topic B: PC Components

Topic C: Common Connection Interfaces

Topic D: Install Peripheral Devices

Topic E: Troubleshooting Methodology

Labs: 1.1.3; 1.1.5; 1.2.7; 2.5.6;

**Lesson 2: Installing, Configuring, and Troubleshooting Display and Multimedia Devices**

Topic A: Install and Configure Display Devices

Topic B: Troubleshoot Display Devices

Topic C: Install and Configure Multimedia Devices

Labs: 3.12.5; 3.13.7;

**Day 2**

**Lesson 3: Installing, Configuring, and Troubleshooting Storage Devices**

Topic A: Install System Memory

Topic B: Install and Configure Mass Storage Devices

Topic C: Install and Configure Removable Storage

Topic D: Configure RAID

Topic E: Troubleshoot Storage Devices

Lab: 3.8.3; 3.8.7; 3.9.4; 3.9.5; 3.11.4;

**Lesson 4: Installing, Configuring, and Troubleshooting Internal System Components**

Topic A: Install and Upgrade CPUs

Topic B: Configure and Update BIOS/UEFI

Topic C: Install Power Supplies

Topic D: Troubleshoot Internal System Components

Topic E: Configure a Custom PC

Labs: Peripheral - 4.1.3; 4.2.3;

**Lesson 5: Network Infrastructure Concepts**

Topic A: Wired Networks

Topic B: Network Hardware Devices

Topic C: Wireless Networks

Topic D: Internet Connection Types

Topic E: Network Configuration Concepts

Topic F: Network Services

Labs: Wired - 6.2.6; 6.6.5; 6.6.6; 6.8.3; 6.8.4; (build a CAT 5 cable and test)

Labs: Wireless - 7.1.7; 7.1.8; 7.1.9; 7.1.10; 7.3.7; 7.4.4; 7.5.3 (practice questions)

**Day 3**

**Lesson 6: Configuring and Troubleshooting Networks**

Topic A: Configure Network Connection Settings

Topic B: Install and Configure SOHO Networks

Topic C: Configure SOHO Network Security

Topic D: Configure Remote Access

Topic E: Troubleshoot Network Connections

Topic F: Install and Configure IoT Devices

Labs: 6.9.3; 6.9.4; 6.9.5; 6.9.6; 6.10.4; 6.10.5

**Lesson 7: Implementing Client Virtualization and Cloud Computing**

Topic A: Configure Client-Side Virtualization

Topic B: Cloud Computing Concepts

Labs: No labs

**Lesson 8: Supporting and Troubleshooting Laptops**

Topic A: Use Laptop Features

Topic B: Install and Configure Laptop Hardware

Topic C: Troubleshoot Common Laptop Issues

Labs: 9.3.5; 9.3.6; 9.4.5 (practice questions)

**Day 4**

**Lesson 9: Supporting and Troubleshooting Mobile Devices**

Topic A: Mobile Device Types

Topic B: Connect and Configure Mobile Device Accessories

Topic C: Configure Mobile Device Network Connectivity

Topic D: Support Mobile Apps

Topic E: Secure Mobile Devices

Topic F: Troubleshoot Mobile Device Issues

Labs: 9.6.7; 9.7.4;

**Lesson 10: Installing, Configuring, and Troubleshooting Print Devices**

Topic A: Maintain Laser Printers

Topic B: Maintain Inkjet Printers

Topic C: Maintain Impact, Thermal, and 3D Printers

Topic D: Install and Configure Printers

Topic E: Troubleshoot Print Device Issues

Topic F: Install and Configure Imaging Devices

Labs: 4.3.3; 4.5.8; 4.6.4; 4.6.5

Non-Virtual Labs:

Operational Procedures - create and deploy an image using Clonezilla; configure Windows backup;

Capstone Testout - 14.1 - Build a computer from scratch (using our build PC kit); install an OS; connect it to the network; connect it to a printer - using all our devices. (Lab manual will be updated, when instructors have had a chance to build one of the kits). We need an additional kit (# 11) to use for spare parts and troubleshooting.

14.4 - Create a home office network; install and configure a wireless router (using one we provide)

14.6 - Troubleshoot a mobile device

Students need a USB drive for Clonezilla; CD to put the OS on; external hard drives to store/deploy the image.

**Day 5**

**Evaluation Time:** After the last lesson of class, students will be given 20 minutes to log into ACI Learning Learning Portal to access and complete the evaluation for their class.

**Assessment: 1 hour timed assessment (Break for 30 or 60 minute lunch)**

**Assessment Review:** If the assessment score is lower than 70%, after the initial assessment review the student will have option to retake another assessment.

GRADING

In order for students to successfully complete the course, they must meet the course participation/attendance and lab completion requirements. Additionally, students seeking an ACE credit recommendation must score a 70 percent or higher on the final exam. Students who are not seeking an ACE credit recommendation are not required to complete the final exam.

CompTIA A+ Practical Applications 1002

COURSE DESCRIPTION

This course is designed for individuals who have basic computer user skills and who are interested in obtaining a job as an entry-level IT technician. This course is also designed for students who are seeking the CompTIA A+ certification and who want to prepare for the CompTIA A+ Core 2 220-1002 Certification.

To ensure your success in this course you should have experience with basic computer user skills, be able to complete tasks in a Microsoft Windows environment, be able to search for, browse and access information on the Internet and have a basic knowledge of computing concepts.

COURSE OBJECTIVES

* Supporting Operating Systems
* Installing, Configuring and Maintaining Operating Systems
* Maintaining and Troubleshooting Microsoft Windows
* Configuring and Troubleshooting Networks
* Managing Users, Workstations, and Shared Resource
* Security Concepts
* Securing Workstations and Data
* Troubleshooting Workstations Security Issues
* Supporting and Troubleshooting Mobile Devices
* Implementing Operational Procedures

course hours

|  |  |  |
| --- | --- | --- |
| **Number** | **Title** | **Contact Hours** |
| 220-1002 | CompTIA A+ Practical Applications | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for night students.

REQUIRED COURSEWARE

* CompTIA A+ Certification, 220-1002 (ebook from CompTIA)
* ACI Learning Learning Management System Student Portal
* TestOut Test Prep
* Professor Messer Guides
* TestOut Labs and ACI Learning Labs

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs (virtual) and in-class
* Videos
* Assessments

COURSE OUTLINE

**Day 1**

**Introductions/Policy Overview/Course Description**

**Lesson 1: Supporting Operation Systems**

Topic A: Identify Common Operation Systems

Topic B: Use Windows Features and Tools

Lab 12.1.13 – Use System Commands (Core 2 – Operating Systems)

Topic C: Manage Files in Windows

* Lab 11.2.5 – Manage Files (Core 2 – Operating Systems)
* Lab 11.2.9 – Manage Files and Folders (Core 2 – Operating Systems)

Topic D: Manage Disks in Windows

* Lab 5.6.3 – Create Volumes (Core 2 – Operating Systems)
* Lab 5.6.5 – Format Drives (Core 2 – Operating Systems)
* Lab 5.7.5 – Add Space to Existing Volumes (Core 2 – Operating Systems)
* Lab 5.8.4 – Implement Storage Spaces (Core 2 – Operating Systems)
* Lab 5.9.6 – Perform Disk Maintenance (Core 2 – Operating Systems)

Topic E: Manage Devices in Windows

* Lab 4.5.8 – Manage Devices (Core 2 – Software Troubleshooting)
* Lab 4.6.4 – Manage Devices 1 (Core 2 – Software Troubleshooting)
* Lab 4.6.5 – Manage Devices 2 (Core 2 – Software Troubleshooting)

**Lesson 2: Installing, configuring and Maintaining Operating Systems**

Topic A: Configure and Use Linux

* Lab 1.4.4 – Use Shell Commands (Core 2 – Operating Systems)
* Lab 1.4.5 – Shut Down a Linux System (Core 2 – Operating Systems)
* Lab 12.8.5 – Manage Linux Processes (Core 2 – Operating Systems)
* Lab 12.8.5 – Manage Linux Processes (Core 2 – Operating Systems)

Topic B: Configure and Use macOS

Topic C: Install and Upgrade Operation Systems

* Lab 10.3.3 – Prepare Disks for Installation (Core 2 – Operating Systems)
* Lab 10.3.5 – Install an Workstation Image using PXE (Core 2 – Operating Systems)

Topic D: Maintain OSs

* Lab 11.5.6 – Manage the Linux File System (Core 2 – Operating Systems)
* Lab 11.5.7 – Manage Linux File Ownership (Core 2 – Operating Systems)
* Lab 12.11.6 – Back Up the Computer (Core 2 – Operating Systems)
* Lab 12.11.7 – Configure File History (Core 2 – Operating Systems)
* Lab 12.12.3 – Create a Restore Point (Core 2 – Operating Systems)
* Lab 13.6.6 – Configure Windows Defender (Core 2 – Security)

**Lesson 3: Maintaining and Troubleshooting Microsoft Windows**

Topic A: Install and Manger Windows Applications

Topic B: Manage Windows Performance

Topic C: Troubleshoot Windows

**Day 2**

**Lesson 4: Configuring and Troubleshooting Networks**

Topic A: Configure Network Connections Settings

Topic B: Install and Configure SOHO Networks

Topic C: Configure SOHO Network Security

Topic D: Configure Remote Access

Topic E: Troubleshoot Network Connections

**Lesson 5: Managing Users, Workstations, and Shared Resource**

Topic A: Manage Users

* Lab 12.4.6 – Create User Accounts (Core 2 – Operating Systems)
* Lab 12.5.6 – Manage Users and Groups (Core 2 – Operating Systems)

Topic B: Configure Shared Resources

* Lab 11.4.6 – Share and Secure Folders (Core 2 – Security)

Topic C: Configure Active Directory Accounts and Policies

* Lab 12.4.3 – Join a Workstation to a Domain (Core 2 – Operating Systems)
* Lab 12.4.7 – Create OUs (Core 2 – Operating Systems)
* Lab 12.4.8 – Delete OUs (Core 2 – Operating Systems)

**Day 3**

**Lesson 6: Security Concepts**

Topic A: Logical Security Concept

Topic B: Threats and Vulnerabilities

Topic C: Physical Security Measures

**Lesson 7: Securing Workstations and Data**

Topic A: Implement Security Best Practices

* Lab 13.3.6 – Require a Screen Saver Password (Core 2 – Security)
* Lab 13.5.4 – Configure BIOS/UEFI Security (Core 2 – Security)

Topic B: Implement Data Projection Policies

* Lab 11.3.4 – Configure NTFS Permissions (Core 2 – Security)
* Lab 13.8.4 – Configure File Encryption (Core 2 – Security)

Topic C: Project Data during Incident Response

**Lesson 8: Troubleshooting Workstations Security Issues**

Topic A: Detect, Remove and Prevent Malware

Topic B: Troubleshoot Common Workstation Security Issues

**Day 4**

**Lesson 9: Supporting and Troubleshooting Mobile Devices**

Topic A: Secure Mobile Devices

Topic B: Troubleshoot Mobile Devices Issues

**Lesson 10: Implementing Operational Procedures**

Topic A: User Appropriate Safety Procedures

Topic B: Environmental Impacts and Controls

Topic C: Create and Maintain Documentation

* Lab 12.10.4 – Configure Windows Update (Core 2 – Operating Systems)
* Lab 12.10.8 – Update Firmware (Core 2 – Operating Systems)

Topic D: Implement Disaster Prevention and Recovery Methods

* Lab 2.5.6 – Install a UPS (Core 2 – Operational Procedures)

Topic E: Basic Scripting Concepts

Topic F: Professionalism and Communication

**Day 5**

**Evaluation Time:** After the last lesson of class, students will be given 20 minutes to log into ACI Learning Learning Portal to access and complete the evaluation for their class.

**Assessment: 1 hour timed assessment (Break for 30 or 60 minute lunch)**

**Assessment Review:** If the assessment score is lower than 70%, after the initial assessment review the student will have option to retake another assessment.

GRADING

In order for students to successfully complete the course, they must meet the course participation/attendance and lab completion requirements. Additionally, students seeking an ACE credit recommendation must score a 70 percent or higher on the final exam. Students who are not seeking an ACE credit recommendation are not required to complete the final exam.

## Computer User Support Specialist (CUSS)

### Program Description

This program is designed to help individuals get jobs in the technical support and service field as end user support specialists. This program develops the skills required to perform the following job functions:

* The program introduces the principles and core elements of IT service management (ITSM) based on ITIL framework
* Install, configure, upgrade, and maintain PC workstations, focusing on the Windows Operating System.
* Resolve PC, OS, and network connectivity issues and implement security practices.
* Manage, maintain, troubleshoot, basic network infrastructure, describe networking technologies, basic design principles, and adhere to wiring standards.
* Perform compliance and operational security tasks
* Anticipate, identify and prevent threats and vulnerabilities
* Manage application, data and host security
* Perform access control and identity management functions
* Understand basic Cryptography concepts
* Install, configure, upgrade, maintain, and troubleshoot servers.
* Examine server hardware and software, disaster recovery strategies.
* Perform installation, troubleshooting, and management functions in the Windows Client operating system environment.
* Troubleshoot security system issues, such as Encrypting File Systems (EFS) BitLocker Drive Encryption, and file permissions.

### Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| ITIL | ITIL Foundations | 20/20/40 |
| 220-1001 | A+ Essentials | 20/20/0/40 |
| 220-1002 | A+ Practical Applications | 20/20/0/40 |
| N10-007 | Network+ | 20/20/0/40 |
| SY0-601 | Security+ | 20/20/0/40 |

The approximate time required to complete this program is 25 days for day students and 50 nights for evening students.

### Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 25 days. Classes for evening students will be held Mondays through Fridays from 7:00PM to 11:00PM. For day students, an hour lunch break will be taken every day from 11:30AM to 12:30PM with four 10 minutes breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

### Tuition and Fees

Registration: $0  
Tuition: $13,342  
Labs: $533  
Total Tuition Fee: $13,875

### Targeted Job Roles

* End User Support Specialist
* Service Technician
* Technical Support Specialist
* Help Desk Specialist
* Desktop Support Specialist
* Security Administrator

### Subject Descriptions and Syllabi

#### ITIL v4 foundations

course DESCRIPTION

Based on the ITIL best practice service lifecycle methodology, this subject provides a practical understanding of the key concepts, principles, processes, and functions that enable successful IT Service Management (ITSM) provisioning. The course intent is to provide proven practical guidance on how to successfully introduce an integrated IT Service Management framework and how best practices can be adopted and adapted within an organization. It also prepares students for the ITIL Foundation Certification. This is for IT practitioners involved in the strategy, design, implementation and on-going delivery of business-used IT services and for anyone who requires an insight into Service Management best practices.

course OBJECTIVES

Upon completion of the 5-Day ITIL Foundations training, participants will understand:

* Key concepts of ITIL
* Important principles for improving IT operations and project success
* Vital processes and functions
* Practical guidance for applying ITIL to everyday IT project situations
* How to align with business, control costs, and improve IT service quality
* Strategies to balance IT resources

Targeted Job Roles

* IT Professionals with an interest in Service Management

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| ITL-FND | ITIL v4 Foundations | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

ITIL 4 Foundation

Course Developer: Logical Operations

Authors: Patrick Von Schlag ITIL Expert

Laurie Perry

Publish Date2019

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

**Day 1**

Module 1: Introduction

* Introduction/Housekeeping
* Introduction to key ITIL concepts
* IT as a Service
* Introduction to processes and process management
* The Service Lifecycle approach

Module 2: Service Strategy

* Purpose, goal, objectives & Scope
* Value Creation through Services
* Assets - Resources and Capabilities
* Service Strategy - Main activities
* Service Strategy processes
* Service Portfolio management
* Demand management
* Financial management
* Business Relationship Management

**Day 2**

Module 3: Service Design

* Purpose, goal, objectives & Scope
* Service Design processes
* The 4 P's
* Service Design aspects
* Service Catalog Management
* Service Level Management
* Capacity Management
* Availability Management
* IT Service Continuity Management
* Service Portfolio
* Information Security Management
* Supplier management
* Design Coordination

Module 4: Service Transition

* Purpose, goal, objectives & Scope
* Service Transition value to the business
* Technology and architecture in Service Transition
* Service Transition Processes
* Change Management
* The 7 R's of Change Management
* Service Asset and Configuration Management
* Release and Deployment Management
* Knowledge Management

**Day 3**

Module 5: Service Operation

* Purpose, goal, objectives & Scope
* Service Operation definitions
* The Service Desk
* Technical Management
* Application Management
* IT Operations Management
* Service Operations Processes
* Event Management
* Request Fulfillment
* Problem Management
* Access Management

Module 6: Continual Service Improvement

* Purpose, goal, objectives & Scope
* Models and Processes
* The Deming Cycle
* Measurement and metrics
* Continual Service Improvement activities
* Risk management
* Continual Service Improvement interfaces
* Interface with Service Level Management

**Day 4**

* Review of Service Strategy
* Review of Service Design
* Review of Service Transition
* Review of Service Operation
* Review of Continual Service Improvement

**Day 5**

* Certification prep
* Certification Attempt

##### Grading

Grading will be assigned as follows:

* Attendance: 75%
* Exercise Participation: 25%

CompTIA A+ 1001 Essentials

This course will build on the student's existing user-level knowledge and experience with personal computer (PC) hardware to present fundamental skills and concepts that are used on the job. In this course, the student will acquire the essential skills and information needed to install, configure, troubleshoot, upgrade, and perform preventive maintenance on PCs and mobile device hardware.

The CompTIA A+ course can benefit the student in two ways. Whether working in a   
mobile or corporate environment with a high level of face-to-face customer interaction, where client   
communication and client training are important, or in an environment with limited customer   
interaction and an emphasis on hardware activities, this course provides the background knowledge and skills required to be a successful A+ technician.

In this course, the student will install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers, digital devices, and operating systems.

COURSE OBJECTIVES

* Install and configure PC system unit components and peripheral devices.
* Install, configure, and troubleshoot display and multimedia devices.
* Install, configure, and troubleshoot storage devices.
* Install, configure, and troubleshoot internal system components.
* Explain network infrastructure concepts.
* Configure and troubleshoot network connections.
* Implement client virtualization and cloud computing.
* Support and troubleshoot laptops.
* Support and troubleshoot mobile devices.
* Install, configure, and troubleshoot print devices.

Course hours

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Contact Hours** |
| A+ 1001 | CompTIA A+ Essentials | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for night students.

REQUIRED COURSEWARE

* CompTIA A+ Certification, 220-1001 (ebook from CompTIA)
* ACI Learning Learning Management System Student Portal
* TestOut Test Prep
* Professor Messer Guides
* TestOut Labs and ACI Learning Labs

iNSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs (virtual)
* Hand on in-class PC build
* Videos
* Assessments

COURSE Outline

**Day 1**

**Introductions/Policy Overview/Course Description**

**Lesson 1: Installing and Configuring PC Components**

Topic A: Use Appropriate Safety Procedures

Topic B: PC Components

Topic C: Common Connection Interfaces

Topic D: Install Peripheral Devices

Topic E: Troubleshooting Methodology

Labs: 1.1.3; 1.1.5; 1.2.7; 2.5.6;

**Lesson 2: Installing, Configuring, and Troubleshooting Display and Multimedia Devices**

Topic A: Install and Configure Display Devices

Topic B: Troubleshoot Display Devices

Topic C: Install and Configure Multimedia Devices

Labs: 3.12.5; 3.13.7;

**Day 2**

**Lesson 3: Installing, Configuring, and Troubleshooting Storage Devices**

Topic A: Install System Memory

Topic B: Install and Configure Mass Storage Devices

Topic C: Install and Configure Removable Storage

Topic D: Configure RAID

Topic E: Troubleshoot Storage Devices

Lab: 3.8.3; 3.8.7; 3.9.4; 3.9.5; 3.11.4;

**Lesson 4: Installing, Configuring, and Troubleshooting Internal System Components**

Topic A: Install and Upgrade CPUs

Topic B: Configure and Update BIOS/UEFI

Topic C: Install Power Supplies

Topic D: Troubleshoot Internal System Components

Topic E: Configure a Custom PC

Labs: Internal Components - 3.2.5; 3.3.5; 3.4.3; 3.4.4; 3.5.7; 3.6.3; 3.6.4;

Labs: Peripheral - 4.1.3; 4.2.3;

**Lesson 5: Network Infrastructure Concepts**

Topic A: Wired Networks

Topic B: Network Hardware Devices

Topic C: Wireless Networks

Topic D: Internet Connection Types

Topic E: Network Configuration Concepts

Topic F: Network Services

Labs: Wired - 6.2.6; 6.6.5; 6.6.6; 6.8.3; 6.8.4; (build a CAT 5 cable and test)

Labs: Wireless - 7.1.7; 7.1.8; 7.1.9; 7.1.10; 7.3.7; 7.4.4; 7.5.3 (practice questions)

**Day 3**

**Lesson 6: Configuring and Troubleshooting Networks**

Topic A: Configure Network Connection Settings

Topic B: Install and Configure SOHO Networks

Topic C: Configure SOHO Network Security

Topic D: Configure Remote Access

Topic E: Troubleshoot Network Connections

Topic F: Install and Configure IoT Devices

Labs: 6.9.3; 6.9.4; 6.9.5; 6.9.6; 6.10.4; 6.10.5

**Lesson 7: Implementing Client Virtualization and Cloud Computing**

Topic A: Configure Client-Side Virtualization

Topic B: Cloud Computing Concepts

Labs: No labs

**Lesson 8: Supporting and Troubleshooting Laptops**

Topic A: Use Laptop Features

Topic B: Install and Configure Laptop Hardware

Topic C: Troubleshoot Common Laptop Issues

Labs: 9.3.5; 9.3.6; 9.4.5 (practice questions)

**Day 4**

**Lesson 9: Supporting and Troubleshooting Mobile Devices**

Topic A: Mobile Device Types

Topic B: Connect and Configure Mobile Device Accessories

Topic C: Configure Mobile Device Network Connectivity

Topic D: Support Mobile Apps

Topic E: Secure Mobile Devices

Topic F: Troubleshoot Mobile Device Issues

Labs: 9.6.7; 9.7.4;

**Lesson 10: Installing, Configuring, and Troubleshooting Print Devices**

Topic A: Maintain Laser Printers

Topic B: Maintain Inkjet Printers

Topic C: Maintain Impact, Thermal, and 3D Printers

Topic D: Install and Configure Printers

Topic E: Troubleshoot Print Device Issues

Topic F: Install and Configure Imaging Devices

Labs: 4.3.3; 4.5.8; 4.6.4; 4.6.5

Non-Virtual Labs:

Operational Procedures - create and deploy an image using Clonezilla; configure Windows backup;

Capstone Testout - 14.1 - Build a computer from scratch (using our build PC kit); install an OS; connect it to the network; connect it to a printer - using all our devices. (Lab manual will be updated, when instructors have had a chance to build one of the kits). We need an additional kit (# 11) to use for spare parts and troubleshooting.

14.4 - Create a home office network; install and configure a wireless router (using one we provide)

14.6 - Troubleshoot a mobile device

Students need a USB drive for Clonezilla; CD to put the OS on; external hard drives to store/deploy the image.

**Day 5**

**Evaluation Time:** After the last lesson of class, students will be given 20 minutes to log into ACI Learning Learning Portal to access and complete the evaluation for their class.

**Assessment: 1 hour timed assessment (Break for 30 or 60 minute lunch)**

**Assessment Review:** If the assessment score is lower than 70%, after the initial assessment review the student will have option to retake another assessment.

GRADING

In order for students to successfully complete the course, they must meet the course participation/attendance and lab completion requirements. Additionally, students seeking an ACE credit recommendation must score a 70 percent or higher on the final exam. Students who are not seeking an ACE credit recommendation are not required to complete the final exam.

CompTIA A+ Practical Applications 1002

COURSE DESCRIPTION

This course is designed for individuals who have basic computer user skills and who are interested in obtaining a job as an entry-level IT technician. This course is also designed for students who are seeking the CompTIA A+ certification and who want to prepare for the CompTIA A+ Core 2 220-1002 Certification.

To ensure your success in this course you should have experience with basic computer user skills, be able to complete tasks in a Microsoft Windows environment, be able to search for, browse and access information on the Internet and have a basic knowledge of computing concepts.

COURSE OBJECTIVES

* Supporting Operating Systems
* Installing, Configuring and Maintaining Operating Systems
* Maintaining and Troubleshooting Microsoft Windows
* Configuring and Troubleshooting Networks
* Managing Users, Workstations, and Shared Resource
* Security Concepts
* Securing Workstations and Data
* Troubleshooting Workstations Security Issues
* Supporting and Troubleshooting Mobile Devices
* Implementing Operational Procedures

course hours

|  |  |  |
| --- | --- | --- |
| **Number** | **Title** | **Contact Hours** |
| 220-1002 | CompTIA A+ Practical Applications | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for night students.

REQUIRED COURSEWARE

* CompTIA A+ Certification, 220-1002 (ebook from CompTIA)
* ACI Learning Learning Management System Student Portal
* TestOut Test Prep
* Professor Messer Guides
* TestOut Labs and ACI Learning Labs

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs (virtual) and in-class
* Videos
* Assessments

COURSE OUTLINE

**Day 1**

**Introductions/Policy Overview/Course Description**

**Lesson 1: Supporting Operation Systems**

Topic A: Identify Common Operation Systems

Topic B: Use Windows Features and Tools

Lab 12.1.13 – Use System Commands (Core 2 – Operating Systems)

Topic C: Manage Files in Windows

* Lab 11.2.5 – Manage Files (Core 2 – Operating Systems)
* Lab 11.2.9 – Manage Files and Folders (Core 2 – Operating Systems)

Topic D: Manage Disks in Windows

* Lab 5.6.3 – Create Volumes (Core 2 – Operating Systems)
* Lab 5.6.5 – Format Drives (Core 2 – Operating Systems)
* Lab 5.7.5 – Add Space to Existing Volumes (Core 2 – Operating Systems)
* Lab 5.8.4 – Implement Storage Spaces (Core 2 – Operating Systems)
* Lab 5.9.6 – Perform Disk Maintenance (Core 2 – Operating Systems)

Topic E: Manage Devices in Windows

* Lab 4.5.8 – Manage Devices (Core 2 – Software Troubleshooting)
* Lab 4.6.4 – Manage Devices 1 (Core 2 – Software Troubleshooting)
* Lab 4.6.5 – Manage Devices 2 (Core 2 – Software Troubleshooting)

**Lesson 2: Installing, configuring and Maintaining Operating Systems**

Topic A: Configure and Use Linux

* Lab 1.4.4 – Use Shell Commands (Core 2 – Operating Systems)
* Lab 1.4.5 – Shut Down a Linux System (Core 2 – Operating Systems)
* Lab 12.8.5 – Manage Linux Processes (Core 2 – Operating Systems)
* Lab 12.8.5 – Manage Linux Processes (Core 2 – Operating Systems)

Topic B: Configure and Use macOS

Topic C: Install and Upgrade Operation Systems

* Lab 10.3.3 – Prepare Disks for Installation (Core 2 – Operating Systems)
* Lab 10.3.5 – Install an Workstation Image using PXE (Core 2 – Operating Systems)

Topic D: Maintain OSs

* Lab 11.5.6 – Manage the Linux File System (Core 2 – Operating Systems)
* Lab 11.5.7 – Manage Linux File Ownership (Core 2 – Operating Systems)
* Lab 12.11.6 – Back Up the Computer (Core 2 – Operating Systems)
* Lab 12.11.7 – Configure File History (Core 2 – Operating Systems)
* Lab 12.12.3 – Create a Restore Point (Core 2 – Operating Systems)
* Lab 13.6.6 – Configure Windows Defender (Core 2 – Security)

**Lesson 3: Maintaining and Troubleshooting Microsoft Windows**

Topic A: Install and Manger Windows Applications

Topic B: Manage Windows Performance

Topic C: Troubleshoot Windows

**Day 2**

**Lesson 4: Configuring and Troubleshooting Networks**

Topic A: Configure Network Connections Settings

Topic B: Install and Configure SOHO Networks

Topic C: Configure SOHO Network Security

Topic D: Configure Remote Access

Topic E: Troubleshoot Network Connections

**Lesson 5: Managing Users, Workstations, and Shared Resource**

Topic A: Manage Users

* Lab 12.4.6 – Create User Accounts (Core 2 – Operating Systems)
* Lab 12.5.6 – Manage Users and Groups (Core 2 – Operating Systems)

Topic B: Configure Shared Resources

* Lab 11.4.6 – Share and Secure Folders (Core 2 – Security)

Topic C: Configure Active Directory Accounts and Policies

* Lab 12.4.3 – Join a Workstation to a Domain (Core 2 – Operating Systems)
* Lab 12.4.7 – Create OUs (Core 2 – Operating Systems)
* Lab 12.4.8 – Delete OUs (Core 2 – Operating Systems)

**Day 3**

**Lesson 6: Security Concepts**

Topic A: Logical Security Concept

Topic B: Threats and Vulnerabilities

Topic C: Physical Security Measures

**Lesson 7: Securing Workstations and Data**

Topic A: Implement Security Best Practices

* Lab 13.3.6 – Require a Screen Saver Password (Core 2 – Security)
* Lab 13.5.4 – Configure BIOS/UEFI Security (Core 2 – Security)

Topic B: Implement Data Projection Policies

* Lab 11.3.4 – Configure NTFS Permissions (Core 2 – Security)
* Lab 13.8.4 – Configure File Encryption (Core 2 – Security)

Topic C: Project Data during Incident Response

**Lesson 8: Troubleshooting Workstations Security Issues**

Topic A: Detect, Remove and Prevent Malware

Topic B: Troubleshoot Common Workstation Security Issues

**Day 4**

**Lesson 9: Supporting and Troubleshooting Mobile Devices**

Topic A: Secure Mobile Devices

Topic B: Troubleshoot Mobile Devices Issues

**Lesson 10: Implementing Operational Procedures**

Topic A: User Appropriate Safety Procedures

Topic B: Environmental Impacts and Controls

Topic C: Create and Maintain Documentation

* Lab 12.10.4 – Configure Windows Update (Core 2 – Operating Systems)
* Lab 12.10.8 – Update Firmware (Core 2 – Operating Systems)

Topic D: Implement Disaster Prevention and Recovery Methods

* Lab 2.5.6 – Install a UPS (Core 2 – Operational Procedures)

Topic E: Basic Scripting Concepts

Topic F: Professionalism and Communication

**Day 5**

**Evaluation Time:** After the last lesson of class, students will be given 20 minutes to log into ACI Learning Learning Portal to access and complete the evaluation for their class.

**Assessment: 1 hour timed assessment (Break for 30 or 60 minute lunch)**

**Assessment Review:** If the assessment score is lower than 70%, after the initial assessment review the student will have option to retake another assessment.

GRADING

In order for students to successfully complete the course, they must meet the course participation/attendance and lab completion requirements. Additionally, students seeking an ACE credit recommendation must score a 70 percent or higher on the final exam. Students who are not seeking an ACE credit recommendation are not required to complete the final exam.

### CompTIA Network +

PROGRAM DESCRIPTION

The *CompTIA® Network+®* course builds on your existing user-level knowledge and experience with personal computer operating systems and networks to present the fundamental skills and concepts that you will need to use on the job in any type of networking career. If you are pursuing a CompTIA technical certification path, the CompTIA A+ certification is an excellent first step to take before preparing for the CompTIA Network+ certification.

 Also, if your job duties include network troubleshooting, installation, or maintenance, or if you are preparing for any type of network-related career, it provides the background knowledge and skills you will require to be successful.

PERFORMANCE OBJECTIVES

Students will learn:

* Identify basic network theory concepts and major network communications methods.
* Describe bounded network media.
* Identify unbounded network media.
* Identify the major types of network implementations.
* Identify TCP/IP addressing and data delivery methods.
* Implement routing technologies.
* Identify the major services deployed on TCP/IP networks.
* Identify the infrastructure of a WAN implementation.
* Identify the components used in cloud computing and virtualization.
* Describe basic concepts related to network security.
* Prevent security breaches.
* Respond to security incidents.
* Identify the components of a remote network implementation.
* Identify the tools, methods, and techniques used in managing a network.
* Describe troubleshooting of issues on a network.

Targeted Job Roles

* Entry-level IT Professional

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* Professional Helpdesk or Computer Support Experience
* CompTIA A+ Certification is helpful but not required

Class Schedule

Day students will attend weekday classes from 8:00AM to 5:00PM for five days. Classes for evening students will be held Monday through Friday from 7:00 PM to 11:00PM. For day students, an hour lunch break will be taken every day from 11:30AM to 12:30PM with four 10 minute breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

subject hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| N10-007 | CompTIA Network + | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

CompTIA Network+ N10-007

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 3/3/20

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM OUTLINE

**Day 1:**

**Chapter 1: Fundamentals**

* Module A: Networking concepts
* Module B: Classifying networks
* Module C: Network models
* Module D: The troubleshooting process

**Chapter 2: Physical networks**

* Module A: Connection technologies
* Module B: Network devices
* Module C: Copper media
* Module D: Optical media
* Module E: Ethernet standards

**Day 2:**

**Chapter 3: TCP/IP networks**

* Module A: IP addressing
* Module B: Core protocols
* Module C: Network ports and applications

**Chapter 4: Internetworking**

* Module A: Switching
* Module B: Routing

**Chapter 5: Wireless LANs**

* Module A: Wireless networks
* Module B: Wireless LAN standards

**Day 3:**

**Chapter 6: Wide area networks**

* Module A: Internet connections
* Module B: WAN infrastructure

**Chapter 7: Cybersecurity principles**

* Module A: Goals and threats
* Module B: Digital security
* Module C: Transport encryption

**Day 4:**

**Chapter 8: Defending networks**

* Module A: Network security components
* Module B: Network authentication systems
* Module C: Hardening networks

**Chapter 9: Evolving network technologies**

* Module A: Network convergence
* Module B: Virtual and cloud systems

**Day 5:**

**Chapter 10: Network operations**

* Module A: Monitoring and optimization
* Module B: Fault tolerance and disaster recovery
* Module C: Incident response

**Chapter 11: Network planning**

* Module A: Network policy design
* Module B: Network installation
* Module C: Maintenance and upgrades

GRADING

Grading will be assigned as follows:

* Attendance: 50%
* Participation: 50%

### CompTIA security +

PROGRAM DESCRIPTION

CompTIA® Security+® (SY0-601) is the primary course you will need to take if your job responsibilities include securing network services, operations and Incident response, governance, Risk and compliance, protecting against attacks, threats and vulnerabilities in your organization. This course prepares you for the CompTIA Security+ certification. In this course, you will build on your knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network. This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (SY0-601) certification, this course can be a significant part of your preparation. However, certification is not the only key to professional success in the field of computer security. 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.

PERFORMANCE OBJECTIVES

Upon completion of this course, students will be able to:

* Identify the fundamental components of information security
* Analyze risk.
* Identify various threats to information security.
* Conduct security assessments to detect vulnerabilities.
* Implement security for hosts and software.
* Implement security for networks.
* Manage identity and access.
* Implement cryptographic solutions in the organization.
* Implement security at the operational level.
* Address security incidents.
* Ensure the continuity of business operations in the event of an incident.

Targeted Job Roles

* IT Security Professionals

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* CompTIA A+ Certification is helpful but not required
* a fundamental understanding of computer and networking concepts
* six to nine months of helpdesk experience recommended

Class Schedule

Day students will attend weekday classes from 8:00AM to 5:00PM for five days. Classes for evening students will be held Monday through Friday from 6:00 PM to 10:00 PM. For day students, a half hour lunch break will be taken every day from 12:00PM to 12:30PM with four 10 minute breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

subject hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| SY0-601 | CompTIA Security + | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for night students.

REQUIRED TEXTBOOK

CompTIA Security+ SYO-601

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 11/12/2020

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM OUTLINE

**Day 1:**

**Chapter 1:** **Comparing Security Roles and Security Controls**

* Topic 1A: Compare and Contrast Information Security Roles
* Topic 1B: Compare and Contrast Security Control and Framework Types

**Chapter 2:**  **Explaining Threat Actors and Threat Intelligence**

* Topic 2A: Explain Threat Actor Types and Attack Vectors
* Topic 2B: Explain Threat Intelligence Sources**Understanding attacks**

**Day 2:**

**Chapter 3: Performing Security Assessments**

* Topic 3A: Assess Organizational Security with Network Reconnaissance Tools
* Topic 3B: Explain Security Concerns with General Vulnerability Types
* Topic 3C: Summarize Vulnerability Scanning Techniques
* Topic 3D: Explain Penetration Testing Concepts

**Chapter 4:** **Identifying Social Engineering and Malware**

* Topic 4A: Compare and Contrast Social Engineering Techniques
* Topic 4B: Analyze Indicators of Malware-Based Attacks

**Day 3:**

**Chapter 5:** **Summarizing Basic Cyptographic Ciphers**

* Topic 5A: Compare and Contrast Basic Cyptographic Ciphers o
* Topic 5B: Summarize Cryptographic Modes of Operation
* Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
* Topic 5D: Summarize Other Cryptographic Technologies

**Chapter 6:** **Implementing Public Key Infrastructure**

* Topic 6A: Implement Certificates and Certificate Authorities
* Topic 6B: Implement PKI Management

**Day 4:**

**Chapter 7: Implementing Authentication Controls**

* Topic 7A: Summarize Authentication Design Concepts
* Topic 7B: Implement Knowledge Based Authentication
* Topic 7C: Implement Authentication Technologies
* Topic 7D: Summarize Biometrics Authentication Concepts

**Chapter 8: Implementing a Secure Network Architecture**

* Topic 8A: Implement Identity and Account Types
* Topic 8B: Implement Account Policies
* Topic 8C: Implement Authorization Solutions
* Topic 8D: Explain the importance of Personnel Policies

**Day 5:**

**Chapter 9: Implementing Secure Network Designs**

* Topic 9A: Implement Secure Network Design
* Topic 9B: Implement Secure Switching and Routing
* Topic 9C: Implement Secure Wireless Infrastructure
* Topic 9D: Implements Load Balancers

**Chapter 10: Implementing Network Security Appliances**

* Topic 10A: Implement Firewalls and Proxy Servers
* Topic 10B: Implement Network Security Monitoring
* Topic 10C: Summarize the Use of SIEM

**Day 6:**

**Chapter 11:** **Implementing Secure Network Protocols**

* Topic 11A: Implement Secure Network Operations Protocols
* Topic 11B: Implement Secure Application Protocols
* Topic 11C: Implement Secure Remote Access Protocols

**Chapter 12: Implementing Host Security Solutions**

* Topic 12A: Implement Secure Firmware
* Topic 12B: Implement Endpoint Security
* Topic 12C: Explain Embedded System Security Implications

**Day 7:**

**Lesson 13: Implementing Secure Mobile Solutions**

* Topic 13A: Implementing Mobile Device Management
* Topic 13B: Implement Secure Mobile Device Connections

**Lesson 14: Summarizing Secure Application Concepts**

* Topic 14A: Analyze Indicators of Application Attacks
* Topic 14B: Analyze Indicators of Web Application Attacks
* Topic 14C: Summarize Secure Coding Practices
* Topic 14D: Implement Secure Script Environments
* Topic 14E: Summarize Deployment and Automation Concepts

**Lesson 15: Implementing Secure Cloud Solution**

* Topic 15A: Summarize Secure Cloud and Virtualization Services
* Topic 15B: Apply Cloud Security Solutions
* Topic 15C: Summarize Infrastructure as Code Concepts

**Day 8:**

**Lesson 16: Explaining Data Privacy and Protection Concepts**

* Topic 16A: Explain Privacy and Data Sensitivity Concepts
* Topic 16B: Explain Privacy and Data Protection Controls

**Lesson 17: Performing Incident Response**

* Topic 17A: Summarize Incident Response Procedures
* Topic 17B: Utilize Appropriate Data Sources For Incident Response
* Topic 17C: Apply Mitigation Controls

**Lesson 18: Explaining Digital Forensics**

* Topic 18A: Explain Key Aspects for Digital Forensics Documentation
* Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

**Day 9:**

**Lesson 19: Summarizing Risk Management Concepts**

* Topic 19A: Explain Risk Management Processes and Concepts
* Topic 19B: Explain Business Impact Analysis Concepts

**Lesson 20: Implementing Cybersecurity Resilience**

* Topic 20A: Implement Redundancy Strategies
* Topic 20B: Implement Backup Strategies
* Topic 20C: Implement Cybersecurity Resilience Strategies

**Lesson 21: Explaining Physical Security**

* Topic 21A: Explain the Importance of Physical Site Security Controls
* Topic 21B: Explain the Importance of Physical Host Security Controls

**Day 10:**

• Overall Course Review

* + PBQs CertMaster Learn - Review
  + CertMaster Practice Exam - Review
  + Labs – Review

• ACE Assessment administered (1-hour timed assessment) last day of class only

* Assessment Review: If the assessment score is lower than 70% after the initial assessment review the student will have the option to retake the assessment

• Evaluation Time: Students will be given 20 minutes to access and complete the evaluation for the class

• To be eligible for exam voucher submit CertMaster Practice Exam to Mentor with 85% and above score (after class completion or graduation)

Grading

Grading will be assigned as follows:

* For students to successfully complete the course, they must meet the course participation/attendance and homework completion requirements. Additionally, students seeking an ACE credit recommendation must score a 70 percent or higher on the final assessment.

## Network Support Specialist (NSS)

### Program Description

Network Support Specialist is a certification program for entry-level network engineers that helps maximize investment in foundational networking knowledge and increase the value of an employer's network. Network Support Specialist is for Network Specialists, Network Administrators, and Network Support Engineers with 1-3 years of experience. The CCNA Routing and Switching validates the ability to install, configure, operate, and troubleshoot medium-size routed and switched networks.

### Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

### Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 20 days. Classes for evening students will be held on Mondays through Fridays from 7:00PM to 11:00PM. Night classes run for approximately eight weeks. For day students, an hour lunch break will be taken every day from 11:30AM to 12:30PM with four 10 minutes breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| N10-007 | CompTIA Network+ | 20/20/0/40 |
| SY0-601 | CompTIA Security+ | 20/20/0/40 |
| CCNA 1 | Certified Cisco Network Administrator, CCNA Part 1 | 20/20/0/40 |
| CCNA 2 | Certified Cisco Network Administrator, CCNA Part 2 | 20/20/0/40 |

The approximate time required to complete this program is four weeks for day students and eight weeks for evening students.

### Tuition and Fees

Registration: $0  
Tuition: $11,618  
Labs: $762  
Total Tuition Fee: $12,380

### Targeted Job Roles

* Network Support Technician
* Network Support Specialist
* Network Administrators
* Network Support Engineer

### Subject Descriptions

#### CompTIA Network +

course DESCRIPTION

The *CompTIA® Network+®* course builds on your existing user-level knowledge and experience with personal computer operating systems and networks to present the fundamental skills and concepts that you will need to use on the job in any type of networking career. If you are pursuing a CompTIA technical certification path, the CompTIA A+ certification is an excellent first step to take before preparing for the CompTIA Network+ certification.

 Also, if your job duties include network troubleshooting, installation, or maintenance, or if you are preparing for any type of network-related career, it provides the background knowledge and skills you will require to be successful.

course OBJECTIVES

Students will learn:

* Identify basic network theory concepts and major network communications methods.
* Describe bounded network media.
* Identify unbounded network media.
* Identify the major types of network implementations.
* Identify TCP/IP addressing and data delivery methods.
* Implement routing technologies.
* Identify the major services deployed on TCP/IP networks.
* Identify the infrastructure of a WAN implementation.
* Identify the components used in cloud computing and virtualization.
* Describe basic concepts related to network security.
* Prevent security breaches.
* Respond to security incidents.
* Identify the components of a remote network implementation.
* Identify the tools, methods, and techniques used in managing a network.
* Describe troubleshooting of issues on a network.

Targeted Job Roles

* Entry-level IT Professional

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* Professional Helpdesk or Computer Support Experience
* CompTIA A+ Certification is helpful but not required

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| N10-007 | CompTIA Network + | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

CompTIA Network+ N10-007

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 3/3/20

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

**Day 1:**

**Chapter 1: Fundamentals**

* Module A: Networking concepts
* Module B: Classifying networks
* Module C: Network models
* Module D: The troubleshooting process

**Chapter 2: Physical networks**

* Module A: Connection technologies
* Module B: Network devices
* Module C: Copper media
* Module D: Optical media
* Module E: Ethernet standards

**Day 2:**

**Chapter 3: TCP/IP networks**

* Module A: IP addressing
* Module B: Core protocols
* Module C: Network ports and applications

**Chapter 4: Internetworking**

* Module A: Switching
* Module B: Routing

**Chapter 5: Wireless LANs**

* Module A: Wireless networks
* Module B: Wireless LAN standards

**Day 3:**

**Chapter 6: Wide area networks**

* Module A: Internet connections
* Module B: WAN infrastructure

**Chapter 7: Cybersecurity principles**

* Module A: Goals and threats
* Module B: Digital security
* Module C: Transport encryption

**Day 4:**

**Chapter 8: Defending networks**

* Module A: Network security components
* Module B: Network authentication systems
* Module C: Hardening networks

**Chapter 9: Evolving network technologies**

* Module A: Network convergence
* Module B: Virtual and cloud systems

**Day 5:**

**Chapter 10: Network operations**

* Module A: Monitoring and optimization
* Module B: Fault tolerance and disaster recovery
* Module C: Incident response

**Chapter 11: Network planning**

* Module A: Network policy design
* Module B: Network installation
* Module C: Maintenance and upgrades

GRADING

Grading will be assigned as follows:

* Attendance: 50%
* Participation: 50%

### CompTIA security +

course DESCRIPTION

CompTIA® Security+® (SY0-601) is the primary course you will need to take if your job responsibilities include securing network services, operations and Incident response, governance, Risk and compliance, protecting against attacks, threats and vulnerabilities in your organization. This course prepares you for the CompTIA Security+ certification. In this course, you will build on your knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network. This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (SY0-601) certification, this course can be a significant part of your preparation. However, certification is not the only key to professional success in the field of computer security. 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.

course OBJECTIVES

Students will learn:

* Identify the fundamental components of information security.
* Analyze risk.
* Identify various threats to information security.
* Conduct security assessments to detect vulnerabilities.
* Implement security for hosts and software.
* Implement security for networks.
* Manage identity and access.
* Implement cryptographic solutions in the organization.
* Implement security at the operational level.
* Address security incidents.
* Ensure the continuity of business operations in the event of an incident.

Targeted Job Roles

* IT Security Professionals

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* CompTIA A+ Certification is helpful but not required
* Fundamental understanding of computer and networking concepts
* Six to nine months of helpdesk experience recommended

subject hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| SY0-601 | CompTIA Security + | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for night students.

REQUIRED TEXTBOOK

CompTIA Security+ SYO-601

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 11/12/2020

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

**Day 1:**

**Chapter 1:** **Comparing Security Roles and Security Controls**

* Topic 1A: Compare and Contrast Information Security Roles
* Topic 1B: Compare and Contrast Security Control and Framework Types

**Chapter 2:**  **Explaining Threat Actors and Threat Intelligence**

* Topic 2A: Explain Threat Actor Types and Attack Vectors
* Topic 2B: Explain Threat Intelligence Sources**Understanding attacks**

**Day 2:**

**Chapter 3: Performing Security Assessments**

* Topic 3A: Assess Organizational Security with Network Reconnaissance Tools
* Topic 3B: Explain Security Concerns with General Vulnerability Types
* Topic 3C: Summarize Vulnerability Scanning Techniques
* Topic 3D: Explain Penetration Testing Concepts

**Chapter 4:** **Identifying Social Engineering and Malware**

* Topic 4A: Compare and Contrast Social Engineering Techniques
* Topic 4B: Analyze Indicators of Malware-Based Attacks

**Day 3:**

**Chapter 5:** **Summarizing Basic Cyptographic Ciphers**

* Topic 5A: Compare and Contrast Basic Cyptographic Ciphers o
* Topic 5B: Summarize Cryptographic Modes of Operation
* Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
* Topic 5D: Summarize Other Cryptographic Technologies

**Chapter 6:** **Implementing Public Key Infrastructure**

* Topic 6A: Implement Certificates and Certificate Authorities
* Topic 6B: Implement PKI Management

**Day 4:**

**Chapter 7: Implementing Authentication Controls**

* Topic 7A: Summarize Authentication Design Concepts
* Topic 7B: Implement Knowledge Based Authentication
* Topic 7C: Implement Authentication Technologies
* Topic 7D: Summarize Biometrics Authentication Concepts

**Chapter 8: Implementing a Secure Network Architecture**

* Topic 8A: Implement Identity and Account Types
* Topic 8B: Implement Account Policies
* Topic 8C: Implement Authorization Solutions
* Topic 8D: Explain the importance of Personnel Policies

**Day 5:**

**Chapter 9: Implementing Secure Network Designs**

* Topic 9A: Implement Secure Network Design
* Topic 9B: Implement Secure Switching and Routing
* Topic 9C: Implement Secure Wireless Infrastructure
* Topic 9D: Implements Load Balancers

**Chapter 10: Implementing Network Security Appliances**

* Topic 10A: Implement Firewalls and Proxy Servers
* Topic 10B: Implement Network Security Monitoring
* Topic 10C: Summarize the Use of SIEM

**Day 6:**

**Chapter 11:** **Implementing Secure Network Protocols**

* Topic 11A: Implement Secure Network Operations Protocols
* Topic 11B: Implement Secure Application Protocols
* Topic 11C: Implement Secure Remote Access Protocols

**Chapter 12: Implementing Host Security Solutions**

* Topic 12A: Implement Secure Firmware
* Topic 12B: Implement Endpoint Security
* Topic 12C: Explain Embedded System Security Implications

**Day 7:**

**Lesson 13: Implementing Secure Mobile Solutions**

* Topic 13A: Implementing Mobile Device Management
* Topic 13B: Implement Secure Mobile Device Connections

**Lesson 14: Summarizing Secure Application Concepts**

* Topic 14A: Analyze Indicators of Application Attacks
* Topic 14B: Analyze Indicators of Web Application Attacks
* Topic 14C: Summarize Secure Coding Practices
* Topic 14D: Implement Secure Script Environments
* Topic 14E: Summarize Deployment and Automation Concepts

**Lesson 15: Implementing Secure Cloud Solution**

* Topic 15A: Summarize Secure Cloud and Virtualization Services
* Topic 15B: Apply Cloud Security Solutions
* Topic 15C: Summarize Infrastructure as Code Concepts

**Day 8:**

**Lesson 16: Explaining Data Privacy and Protection Concepts**

* Topic 16A: Explain Privacy and Data Sensitivity Concepts
* Topic 16B: Explain Privacy and Data Protection Controls

**Lesson 17: Performing Incident Response**

* Topic 17A: Summarize Incident Response Procedures
* Topic 17B: Utilize Appropriate Data Sources For Incident Response
* Topic 17C: Apply Mitigation Controls

**Lesson 18: Explaining Digital Forensics**

* Topic 18A: Explain Key Aspects for Digital Forensics Documentation
* Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

**Day 9:**

**Lesson 19: Summarizing Risk Management Concepts**

* Topic 19A: Explain Risk Management Processes and Concepts
* Topic 19B: Explain Business Impact Analysis Concepts

**Lesson 20: Implementing Cybersecurity Resilience**

* Topic 20A: Implement Redundancy Strategies
* Topic 20B: Implement Backup Strategies
* Topic 20C: Implement Cybersecurity Resilience Strategies

**Lesson 21: Explaining Physical Security**

* Topic 21A: Explain the Importance of Physical Site Security Controls
* Topic 21B: Explain the Importance of Physical Host Security Controls

**Day 10:**

• Overall Course Review

* + PBQs CertMaster Learn - Review
  + CertMaster Practice Exam - Review
  + Labs – Review

• ACE Assessment administered (1-hour timed assessment) last day of class only

* Assessment Review: If the assessment score is lower than 70% after the initial assessment review the student will have the option to retake the assessment

• Evaluation Time: Students will be given 20 minutes to access and complete the evaluation for the class

• To be eligible for exam voucher submit CertMaster Practice Exam to Mentor with 85% and above score (after class completion or graduation)

##### Grading

Grading will be assigned as follows:

* For students to successfully complete the course, they must meet the course participation/attendance and homework completion requirements. Additionally, students seeking an ACE credit recommendation must score a 70 percent or higher on the final assessment.

CCNA 1 & 2: Certified Cisco Network Administrator, CCNA

course DESCRIPTION

Cisco Certified Network Associate (CCNA) Routing and Switching is a certification program for entry-level network engineers that helps maximize investment in foundational networking knowledge and increase the value of an employer's network. CCNA Routing and Switching is for Network Specialists, Network Administrators, and Network Support Engineers with 1-3 years of experience. The CCNA Routing and Switching validates the ability to install, configure, operate, and troubleshoot medium-size routed and switched networks.

course OBJECTIVES

In this course, you will implement and administer networks by using Cisco solutions.

You will:

* Explain basic concepts related to networking.
* Configure switching.
* Configure IP addressing.
* Configure routing.
* Configure wireless connectivity.
* Configure IP network services.
* Explain basic network security concepts and practices.
* Explain the use of automation and programmability in network management tasks.
* Troubleshoot common network issues.

Targeted Job Roles

* Systems Administrators
* Networking Specialists

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| CCNA 1 | Certified Cisco Network Administrator, CCNA Part 1 Prep | 20/20/0/40 |
| CCNA 2 | Certified Cisco Network Administrator, CCNA Part 2 Prep | 20/20/0/40 |

The approximate time required to complete this program is ten days for day students and twenty nights for evening students.

REQUIRED TEXTBOOK

Logical Operations

CCENT

093042SC (Rev 1.0)

Print and Digital Courseware

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

* Lesson 1: Networking Fundamentals
* Topic A: Network Types
* Topic B: Network Components
* Topic C: Network Topologies
* Topic D: Network Models
* Topic E: Basic Networking Protocols
* Topic F: Transmission Media and Connectors
* Topic G: Introduction to Cisco Networks and Cisco IOS Commands
* Lesson 2: Configuring Switching
* Topic A: Switching Concepts
* Topic B: Configure Basic Switch Operation
* Topic C: Configure VLANs
* Topic D: Configure Interswitch Connectivity
* Lesson 3: Configuring IP Addressing
* Topic A: Configure IPv4 Addresses
* Topic B: Configure IPv4 Subnets
* Topic C: Configure IPv6 Addresses
* Topic D: Manage Network Addressing
* Lesson 4: Configuring Routing
* Topic A: Routing Basics
* Topic B: Interpret Routing Tables
* Topic C: Configure Static Routing
* Topic D: Configure Dynamic Routing
* Lesson 5: Configuring Wireless Connectivity
* Topic A: Wireless LANs
* Topic B: Manage WLAN Connections
* Topic C: Configure Clients for WLAN Access
* Lesson 6: Configuring IP Network Services
* Topic A: IP Network Services
* Topic B: Configure DHCP
* Topic C: Configure NAT
* Topic D: Configure NTP
* Topic E: Configure DNS
* Topic F: Perform Network Management
* Lesson 7: Security Fundamentals
* Topic A: Security Concepts
* Topic B: Manage Passwords
* Topic C: Configure Layer 2 Security
* Topic D: Configure Wireless Security
* Topic E: Remote Access Security
* Lesson 8: Automation and Programmability
* Topic A: Automation, Network Management, and Device Management
* Topic B: Controller-Based Networking and Software-Defined Networking
* Topic C: Programmability Concepts
* Lesson 9: Troubleshooting Network Issues
* Topic A: Troubleshooting Methodologies
* Topic B: Troubleshoot Interface and Cable Issues
* Topic C: Troubleshoot Switching Issues
* Topic D: Troubleshoot IPv4 and IPv6 Addressing Issues
* Topic E: Troubleshoot Routing Issues
* Topic F: Troubleshoot WLAN Issues
* Topic G: Troubleshoot Network Services Issues
* Topic H: Troubleshoot Network Management Issues
* Topic I: Troubleshoot Security Issues

## CCNA

### Program Description

The Cisco® Solutions: Implementation and Administration (CCNA 200-301) course builds on your existing user-level knowledge and experience with computing and networking to provide you with the knowledge and skills expected of an entry-level network administrator. It also addresses the content described in the exam objectives for the Certified Cisco Network Administrator (CCNA® 200-301). If you are pursuing a Cisco technical certification path, the CCNA 200.301 exam is your first step into the world of Cisco certification.

### Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| CCNA 1 | Certified Cisco Network Administrator, CCNA Part 1 Prep | 20/20/0/40 |
| CCNA 2 | Certified Cisco Network Administrator, CCNA Part 2 Prep | 20/20/0/40 |

The approximate time required to complete this program is two weeks for day students and four weeks for evening students.

### Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for ten days. Classes for evening students will be held on Mondays through Fridays from 7:00PM to 11:00PM. Night classes run for approximately four weeks. For day students, an hour lunch break will be taken every day from 11:30AM to 12:30PM with four 10 minutes breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

### Tuition and Fees

Registration: $0  
Tuition: $6,192  
Labs: $398  
Total Tuition Fee: $6,590

### Targeted Job Roles

* Network Specialist
* Network Administrators
* Network Support Engineer

### Subject Descriptions

CCNA 1 & 2: Certified Cisco Network Administrator, CCNA

course DESCRIPTION

Cisco Certified Network Associate (CCNA) Routing and Switching is a certification program for entry-level network engineers that helps maximize investment in foundational networking knowledge and increase the value of an employer's network. CCNA Routing and Switching is for Network Specialists, Network Administrators, and Network Support Engineers with 1-3 years of experience. The CCNA Routing and Switching validates the ability to install, configure, operate, and troubleshoot medium-size routed and switched networks.

course OBJECTIVES

In this course, you will implement and administer networks by using Cisco solutions.

You will:

* Explain basic concepts related to networking.
* Configure switching.
* Configure IP addressing.
* Configure routing.
* Configure wireless connectivity.
* Configure IP network services.
* Explain basic network security concepts and practices.
* Explain the use of automation and programmability in network management tasks.
* Troubleshoot common network issues.

Targeted Job Roles

* Systems Administrators
* Networking Specialists

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| CCNA 1 | Certified Cisco Network Administrator, CCNA Part 1 | 20/20/0/40 |
| CCNA 2 | Certified Cisco Network Administrator, CCNA Part 2 | 20/20/0/40 |

The approximate time required to complete this program is ten days for day students and twenty nights for evening students.

REQUIRED TEXTBOOK

Logical Operations

CCENT

093042SC (Rev 1.0)

Print and Digital Courseware

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

* Lesson 1: Networking Fundamentals
* Topic A: Network Types
* Topic B: Network Components
* Topic C: Network Topologies
* Topic D: Network Models
* Topic E: Basic Networking Protocols
* Topic F: Transmission Media and Connectors
* Topic G: Introduction to Cisco Networks and Cisco IOS Commands
* Lesson 2: Configuring Switching
* Topic A: Switching Concepts
* Topic B: Configure Basic Switch Operation
* Topic C: Configure VLANs
* Topic D: Configure Interswitch Connectivity
* Lesson 3: Configuring IP Addressing
* Topic A: Configure IPv4 Addresses
* Topic B: Configure IPv4 Subnets
* Topic C: Configure IPv6 Addresses
* Topic D: Manage Network Addressing
* Lesson 4: Configuring Routing
* Topic A: Routing Basics
* Topic B: Interpret Routing Tables
* Topic C: Configure Static Routing
* Topic D: Configure Dynamic Routing
* Lesson 5: Configuring Wireless Connectivity
* Topic A: Wireless LANs
* Topic B: Manage WLAN Connections
* Topic C: Configure Clients for WLAN Access
* Lesson 6: Configuring IP Network Services
* Topic A: IP Network Services
* Topic B: Configure DHCP
* Topic C: Configure NAT
* Topic D: Configure NTP
* Topic E: Configure DNS
* Topic F: Perform Network Management
* Lesson 7: Security Fundamentals
* Topic A: Security Concepts
* Topic B: Manage Passwords
* Topic C: Configure Layer 2 Security
* Topic D: Configure Wireless Security
* Topic E: Remote Access Security
* Lesson 8: Automation and Programmability
* Topic A: Automation, Network Management, and Device Management
* Topic B: Controller-Based Networking and Software-Defined Networking
* Topic C: Programmability Concepts
* Lesson 9: Troubleshooting Network Issues
* Topic A: Troubleshooting Methodologies
* Topic B: Troubleshoot Interface and Cable Issues
* Topic C: Troubleshoot Switching Issues
* Topic D: Troubleshoot IPv4 and IPv6 Addressing Issues
* Topic E: Troubleshoot Routing Issues
* Topic F: Troubleshoot WLAN Issues
* Topic G: Troubleshoot Network Services Issues
* Topic H: Troubleshoot Network Management Issues
* Topic I: Troubleshoot Security Issues

GRADING

Grading will be assigned as follows:

* Attendance: 50%
* Participation: 50%

## Information Security Analyst (ISA)

Program Description

CompTIA Security+ SY0-601 certification, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field.

CND prepares individuals on network security technologies and operations to achieve defense-in-depth objectives. CND is a comprehensive vendor-neutral network security certification course. This subject will immerse you into an interactive environment where you will learn and practice security skills. This class also prepares you for EC-Council Certified Network Defender exam 312-38.

CEH will immerse you into an interactive environment where you will be shown how to scan, test, hack and secure your own systems. The lab intensive environment gives you in-depth knowledge and practical experience with the current essential security systems. You will begin by understanding how perimeter defenses work and then be led into scanning and attacking your own networks, no real network is harmed. You will then learn how intruders escalate privileges and what steps can be taken to secure a system. You will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When you leaves this intensive 5 day class, you will have hands on understanding and experience in Ethical Hacking. This class also prepares you for EC-Council ANSI accredited Certified Ethical Hacker exam 312-50.

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| SY0-601 | Security+ | 20/20/0/40 |
| CND | Network Defender | 20/20/0/40 |
| CEH | Professional Ethical Hacker | 20/20/0/40 |

The approximate time required to complete this program is three weeks for day students and six weeks for evening students.

Class Schedule

Day students will attend weekday classes from 8:00AM to 5:00PM for five days. Classes for evening students will be held Monday through Friday from 7:00 PM to 11:00PM. For day students, an hour lunch break will be taken every day from 11:30AM to 12:30PM with four 10 minute breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

Tuition and Fees

Registration: $0  
Tuition: $9,432  
Labs: $1,053  
Total Tuition Fee: $10,485

Targeted Job Roles

* Network Administrator
* Network Engineer
* Information Security Specialist
* Information Security Auditor
* Site Security Administrator

Subject Descriptions

### CompTIA security +

course DESCRIPTION

CompTIA® Security+® (SY0-601) is the primary course you will need to take if your job responsibilities include securing network services, operations and Incident response, governance, Risk and compliance, protecting against attacks, threats and vulnerabilities in your organization. This course prepares you for the CompTIA Security+ certification. In this course, you will build on your knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network. This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (SY0-601) certification, this course can be a significant part of your preparation. However, certification is not the only key to professional success in the field of computer security. 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.

course OBJECTIVES

Students will learn:

* Identify the fundamental components of information security.
* Analyze risk.
* Identify various threats to information security.
* Conduct security assessments to detect vulnerabilities.
* Implement security for hosts and software.
* Implement security for networks.
* Manage identity and access.
* Implement cryptographic solutions in the organization.
* Implement security at the operational level.
* Address security incidents.
* Ensure the continuity of business operations in the event of an incident.

Targeted Job Roles

* IT Security Professionals

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* CompTIA A+ Certification is helpful but not required
* a fundamental understanding of computer and networking concepts
* six to nine months of helpdesk experience recommended

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| SY0-601 | CompTIA Security + | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

CompTIA Security+ SYO-601

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 11/12/2020

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

**Day 1:**

**Chapter 1:** **Comparing Security Roles and Security Controls**

* Topic 1A: Compare and Contrast Information Security Roles
* Topic 1B: Compare and Contrast Security Control and Framework Types

**Chapter 2:**  **Explaining Threat Actors and Threat Intelligence**

* Topic 2A: Explain Threat Actor Types and Attack Vectors
* Topic 2B: Explain Threat Intelligence Sources**Understanding attacks**

**Day 2:**

**Chapter 3: Performing Security Assessments**

* Topic 3A: Assess Organizational Security with Network Reconnaissance Tools
* Topic 3B: Explain Security Concerns with General Vulnerability Types
* Topic 3C: Summarize Vulnerability Scanning Techniques
* Topic 3D: Explain Penetration Testing Concepts

**Chapter 4:** **Identifying Social Engineering and Malware**

* Topic 4A: Compare and Contrast Social Engineering Techniques
* Topic 4B: Analyze Indicators of Malware-Based Attacks

**Day 3:**

**Chapter 5:** **Summarizing Basic Cyptographic Ciphers**

* Topic 5A: Compare and Contrast Basic Cyptographic Ciphers o
* Topic 5B: Summarize Cryptographic Modes of Operation
* Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
* Topic 5D: Summarize Other Cryptographic Technologies

**Chapter 6:** **Implementing Public Key Infrastructure**

* Topic 6A: Implement Certificates and Certificate Authorities
* Topic 6B: Implement PKI Management

**Day 4:**

**Chapter 7: Implementing Authentication Controls**

* Topic 7A: Summarize Authentication Design Concepts
* Topic 7B: Implement Knowledge Based Authentication
* Topic 7C: Implement Authentication Technologies
* Topic 7D: Summarize Biometrics Authentication Concepts

**Chapter 8: Implementing a Secure Network Architecture**

* Topic 8A: Implement Identity and Account Types
* Topic 8B: Implement Account Policies
* Topic 8C: Implement Authorization Solutions
* Topic 8D: Explain the importance of Personnel Policies

**Day 5:**

**Chapter 9: Implementing Secure Network Designs**

* Topic 9A: Implement Secure Network Design
* Topic 9B: Implement Secure Switching and Routing
* Topic 9C: Implement Secure Wireless Infrastructure
* Topic 9D: Implements Load Balancers

**Chapter 10: Implementing Network Security Appliances**

* Topic 10A: Implement Firewalls and Proxy Servers
* Topic 10B: Implement Network Security Monitoring
* Topic 10C: Summarize the Use of SIEM

**Day 6:**

**Chapter 11:** **Implementing Secure Network Protocols**

* Topic 11A: Implement Secure Network Operations Protocols
* Topic 11B: Implement Secure Application Protocols
* Topic 11C: Implement Secure Remote Access Protocols

**Chapter 12: Implementing Host Security Solutions**

* Topic 12A: Implement Secure Firmware
* Topic 12B: Implement Endpoint Security
* Topic 12C: Explain Embedded System Security Implications

**Day 7:**

**Lesson 13: Implementing Secure Mobile Solutions**

* Topic 13A: Implementing Mobile Device Management
* Topic 13B: Implement Secure Mobile Device Connections

**Lesson 14: Summarizing Secure Application Concepts**

* Topic 14A: Analyze Indicators of Application Attacks
* Topic 14B: Analyze Indicators of Web Application Attacks
* Topic 14C: Summarize Secure Coding Practices
* Topic 14D: Implement Secure Script Environments
* Topic 14E: Summarize Deployment and Automation Concepts

**Lesson 15: Implementing Secure Cloud Solution**

* Topic 15A: Summarize Secure Cloud and Virtualization Services
* Topic 15B: Apply Cloud Security Solutions
* Topic 15C: Summarize Infrastructure as Code Concepts

**Day 8:**

**Lesson 16: Explaining Data Privacy and Protection Concepts**

* Topic 16A: Explain Privacy and Data Sensitivity Concepts
* Topic 16B: Explain Privacy and Data Protection Controls

**Lesson 17: Performing Incident Response**

* Topic 17A: Summarize Incident Response Procedures
* Topic 17B: Utilize Appropriate Data Sources For Incident Response
* Topic 17C: Apply Mitigation Controls

**Lesson 18: Explaining Digital Forensics**

* Topic 18A: Explain Key Aspects for Digital Forensics Documentation
* Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

**Day 9:**

**Lesson 19: Summarizing Risk Management Concepts**

* Topic 19A: Explain Risk Management Processes and Concepts
* Topic 19B: Explain Business Impact Analysis Concepts

**Lesson 20: Implementing Cybersecurity Resilience**

* Topic 20A: Implement Redundancy Strategies
* Topic 20B: Implement Backup Strategies
* Topic 20C: Implement Cybersecurity Resilience Strategies

**Lesson 21: Explaining Physical Security**

* Topic 21A: Explain the Importance of Physical Site Security Controls
* Topic 21B: Explain the Importance of Physical Host Security Controls

**Day 10:**

• Overall Course Review

* + PBQs CertMaster Learn - Review
  + CertMaster Practice Exam - Review
  + Labs – Review

• ACE Assessment administered (1-hour timed assessment) last day of class only

* Assessment Review: If the assessment score is lower than 70% after the initial assessment review the student will have the option to retake the assessment

• Evaluation Time: Students will be given 20 minutes to access and complete the evaluation for the class

• To be eligible for exam voucher submit CertMaster Practice Exam to Mentor with 85% and above score (after class completion or graduation)

### CERTIFIED NETWORK DEFENDER (CND)

course DESCRIPTION

The Certified Network Defender (CND) cyber security training program was developed as a result of extensive market research and surveys to give students a detailed understanding and the hands-on ability to act in real-life situations involving network defense.

This course instructs entry and junior level network security administrators on Defense-in-Depth network security preparedness. It covers the *protect, detect, and respond* approach to network security. Hands-on labs, based on major network security tools and techniques, give network administrators real world experience on current network security technologies and operations.

The included study kit provides over 10 GB of network security best practices, assessments, and protection tools. The kit also contains templates for various network policies and several white papers for additional learning.

This cyber security training is skills-based and lab intensive. It based on a job-task analysis and the cyber security education framework presented by the National Initiative of Cybersecurity Education (NICE). The course has been mapped to global job roles and responsibilities and the Department of Defense (DoD) job roles for system and network administrators.

The CND cyber security certification will verify that students have the technical depth required to actively design, monitor, and defend a secure network for an organization.

course OBJECTIVES

Students will learn:

* Various network security controls, protocols, and devices
* How to determine appropriate location for IDS/IPS sensors, tuning IDS for false positives and false negatives, and configurations to harden security through IDPS technologies
* How to implement secure VPNs for their organization
* How to identify various threats to wireless networks and learn how to mitigate them
* How to monitor and conduct signature analysis to detect various types of attacks and policy violation activities
* How to perform risk assessment, vulnerability assessment/scanning through various scanning tools and generate detailed reports on it
* How to identify the critical data, choose appropriate back up method, media and technique to perform successful backup of organization data on regular basis
* How to provide first response to the network security incident and assist IRT team and forensics investigation team in dealing with an incident
* How to troubleshoot their network for various network problems
* How to identify various threats on organization network
* How to design and implement various security policies for their organizations
* The importance of physical security and able to determine and implement various physical security controls for their organizations
* How to harden security of various hosts individually in the organization’s network
* How to choose appropriate firewall solutions, topology, and configurations to harden security through firewall

Targeted Job Roles

* Entry Level Network Administrators
* Entry Level Network Security Administrators
* Junior Network Security Engineers
* Junior Network Defense Technicians
* Security Analysts
* Security Operators

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* Basic IP addressing knowledge
* Computer security knowledge and skills

course hours

|  |  |  |
| --- | --- | --- |
| Subject Number | Subject Title | Contact Hours |
| CND | Certified Network Defender | 40 |

The approximate time required to complete this program is five days for day students and 10 nights for night students.

REQUIRED TEXTBOOK

Certified Network Defender Volume 1  
EC-Council Official Courseware  
Includes: 3 Books (Courseware and Lab Manual) & Tools (Downloadable Online and Instruction provided in the Courseware)

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Lab Exercises

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course Outline

Day 1

* Computer Network Defense Fundamentals
* Network Security Threats, Vulnerabilities, and Attacks
* Network Security Controls, Protocols, and Perimeter Appliances
* Secure Firewall Configuration, Deployment and Management

Day 2

* Secure IDS Configuration and Management
* Secure VPN Configuration and Management
* Designing a Secure Network
* Network Traffic Signatures and Analysis

Day 3

* Monitoring and Securing Network Traffic
* Network Vulnerability Scanning
* Monitoring and Securing Network Traffic
* Network Vulnerability Scanning

Day 4

* Host/System Security
* Physical Security
* Designing and Implementation of Network Security Policies

Day 5

* Network Incident Response and Management
* Network Backup and Disaster Recovery
* Wireless Network Defense

Grading

Grading will be assigned as follows:

-Attendance: 50%

-Lab Assignments: 50%

#### Certified Ethical Hacker (CEH)

course DESCRIPTION

This subject will immerse you into an interactive environment where you will be shown how to scan, test, hack and secure your own systems. The lab intensive environment gives you in-depth knowledge and practical experience with the current essential security systems. You will begin by understanding how perimeter defenses work and then be led into scanning and attacking your own networks, no real network is harmed. You will then learn how intruders escalate privileges and what steps can be taken to secure a system. You will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When you leave this intensive 5 day class, you will have hands on understanding and experience in Ethical Hacking.

course OBJECTIVES

* Students will learn:
* Background of technology and technological operations
* Risk and system analysis
* Systems securities and vulnerabilities
* Regulations and ethics

Targeted Job Roles

* Site Administrators
* Security Auditors
* Security Professionals

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* Basic IP addressing knowledge

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| CEH | Certified Ethical Hacker | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

Certified Ethical Hacker v10

Course Developer: EC-Council

Author: EC-Council approved SME’s

Publish Date: 2018

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

**Lesson 1: Introduction to Ethical Hacking**

* Information Security Overview
* Information Security Threats and Attack Vectors
* Hacking Concepts, Types, and Phases
* Ethical Concepts Hacking and Scopes
* Information Security Controls
* Physical Security
* Information Management
* Vulnerability Assessment
* Penetration Testing
* Security Laws and Standards

**Lesson 2: Footprinting and Reconnaissance**

* Footprinting Concepts
* Footprinting Methodology
* Footprinting Using Advanced Google Hacking Techniques
* Footprinting Tools
* Footprinting Countermeasures
* Footprinting Penetration Testing

**Lesson 3: Scanning Networks**

* Overview of Network Scanning
* CEH Scanning Methodology

**Lesson 4: Enumeration**

* Enumeration Concepts
* Enumerations Countermeasures
* Enumeration Penetration Testing

**Lesson 5: System Hacking**

* System Hacking: Goals
* CEH Hacking: Methodology
* CEH System Hacking Steps
* Escalating Privileges
* Executing Applications
* Spyware
* Defending Against Keyloggers
* Hiding Files
* Detecting Rootkits
* NTFS Data Stream
* Steganography/Steganlysis
* Covering Tracks

**Lesson 6: Malware Threats**

* Trojan Concepts
* Types of Trojans
* Virus and Worm Concepts
* Ransomware
* Malware Reverse Engineering
* Malware Detection
* Countermeasures
* Penetration Testing

**Lesson 7: Sniffing**

* Sniffing Concepts
* MAC/DHCP Attacks
* IDRP Spoofing
* ARP/DNS Poisoning
* Sniffing Tools
* Detection Techniques
* Counter Measures

**Lesson 8: Social Engineering**

* Social Engineering Concepts
* Social Engineering Techniques
* Identity Theft
* Social Engineering Countermeasures

**Lesson 9: Denial of Service**

* DoS/DDoS Concepts
* DoS/DDoS Attack Techniques
* Botnets
* DoS/DDos Attack Tools
* Counter Measures
* DoS/DDos Protection Tools

**Lesson 10: Session Hijacking**

* Session Hijacking Concepts
* Application Level Hijacking
* Network Level Hijacking
* Hijacking Tools
* Countermeasures

**Lesson 11: Hacking Web Servers**

* Webserver Concepts
* Webserver Attakcs
* Attack Methodology
* Webserver Attack Tools
* Patch Management
* Webserver Security Tools

**Lesson 12: Hacking Web Applications**

* Web App Concepts
* Web App Threats
* Web App Hacking Methodology
* Attack Web Servers
* Analyze Web Apps
* Authorization Attack Schemes
* Perform Injection Attacks
* Attack Data Connectivity

**Lesson 13: SQL Injection**

* SQL Injection Concepts
* Types of SQL Injection
* SQL Injection Methodology
* SQL Injection Tools
* Evasion Techniques
* Counter Measures
* Snort Rule Detection to SQL Injection Attacks
* Detection Tools

**Lesson 14: Hacking Wireless Networks**

* Wireless Statistics
* Wireless Concepts
* Wireless Encryption
* Breaking Encryption
* Defending Against WPA Cracking
* Wireless Threats
* Wireless Hacking Methodology
* WEP/WPA Cracking Tools
* Counter Measures
* Security Tools

**Lesson 15: Hacking Mobile Platforms**

* Mobile Platform Attack Vectors
* Hacking Android/IOS
* Hacking Windows/BlackBerry
* Mobile Device Management
* Mobile Security Guidelines and Tools

**Lesson 16: Evading IDS, Firewalls and Honeypots**

* IDS, Firewall and Honeypot Concepts
* IDS, Firewall and Honeypot Systems
* IDS/Firewall Evading Tools
* Detecting Honeypots
* Counter Measures

**Lesson 17: Cloud Computing**

* Introduction to Cloud Computing
* Cloud Computing Threats/Attacks
* Cloud Security
* Cloud Penetration Testing

**Lesson 18: Cryptography**

* Cryptography Concepts
* Encryption Algorithms
* Cryptography Tools
* Public Key Infrastructure
* Email Encryption
* Disk Encryption
* Cryptography Attacks
* Cryptanalysis Tools

GRADING

Grading will be assigned as follows:

* Attendance: 50%
* Participation: 50%

## Cybersecurity Specialist (CYBER)

### Program Description

Battles between corporations, governments, and countries are no longer fought using physical force. Cyber war has begun and the consequences can be seen in everyday life.

This program is designed to help individuals get jobs as information security auditors, site administrators, computer forensics investigators.

This program will immerse the student into an interactive environment where they will be shown how to scan, test, hack and secure their own systems; emphasizing perimeter defenses, Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. It also presents a detailed methodological approach to computer forensics and evidence analysis, covering major forensic investigation scenarios that provide hands-on experience on various forensic investigation techniques and standard tools necessary to successfully carry-out a computer forensic investigation.

### Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score on the ACI Learning Basic Skills Test.

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| SY0-601 | Security+ | 20/20/0/40 |
| CEH | Certified Ethical Hacker | 20/20/0/40 |
| CHFI | Computer Hacking Forensics Investigator | 20/20/0/40 |

The approximate time required to complete this program is three weeks for day students and six weeks for evening students.

### Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 15 days. Classes for evening students will be held on Mondays through Fridays from 7:00PM to 11:00PM. Night classes run for approximately eight weeks. For day students, an hour lunch break will be taken every day from 11:30AM to 12:30PM with four 10 minutes breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

### Tuition and Fees

Registration: $0  
Tuition: $9,432  
Labs: $1,120  
Total Tuition Fee: $10,485

### Targeted Job Roles

* Information Security Specialist
* Information Security Auditor
* Site Security Administrator
* Computer forensics Investigator

### Subject Descriptions and Syllabi

#### CompTIA security +

course DESCRIPTION

CompTIA® Security+® (SY0-601) is the primary course you will need to take if your job responsibilities include securing network services, operations and Incident response, governance, Risk and compliance, protecting against attacks, threats and vulnerabilities in your organization. This course prepares you for the CompTIA Security+ certification. In this course, you will build on your knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network. This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (SY0-601) certification, this course can be a significant part of your preparation. However, certification is not the only key to professional success in the field of computer security. 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.

course OBJECTIVES

Upon completion of this course, students will be able to:

* Identify the fundamental components of information security
* Analyze risk.
* Identify various threats to information security.
* Conduct security assessments to detect vulnerabilities.
* Implement security for hosts and software.
* Implement security for networks.
* Manage identity and access.
* Implement cryptographic solutions in the organization.
* Implement security at the operational level.
* Address security incidents.

Targeted Job Roles

* IT Security Professionals

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* CompTIA A+ Certification is helpful but not required
* Fundamental understanding of computer and networking concepts
* Six to nine months of helpdesk experience recommended

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| SY0-601 | CompTIA Security + | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

CompTIA Security+ SYO-601

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 11/12/2020

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

**Day 1:**

**Chapter 1:** **Comparing Security Roles and Security Controls**

* Topic 1A: Compare and Contrast Information Security Roles
* Topic 1B: Compare and Contrast Security Control and Framework Types

**Chapter 2:**  **Explaining Threat Actors and Threat Intelligence**

* Topic 2A: Explain Threat Actor Types and Attack Vectors
* Topic 2B: Explain Threat Intelligence Sources**Understanding attacks**

**Day 2:**

**Chapter 3: Performing Security Assessments**

* Topic 3A: Assess Organizational Security with Network Reconnaissance Tools
* Topic 3B: Explain Security Concerns with General Vulnerability Types
* Topic 3C: Summarize Vulnerability Scanning Techniques
* Topic 3D: Explain Penetration Testing Concepts

**Chapter 4:** **Identifying Social Engineering and Malware**

* Topic 4A: Compare and Contrast Social Engineering Techniques
* Topic 4B: Analyze Indicators of Malware-Based Attacks

**Day 3:**

**Chapter 5:** **Summarizing Basic Cyptographic Ciphers**

* Topic 5A: Compare and Contrast Basic Cyptographic Ciphers o
* Topic 5B: Summarize Cryptographic Modes of Operation
* Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
* Topic 5D: Summarize Other Cryptographic Technologies

**Chapter 6:** **Implementing Public Key Infrastructure**

* Topic 6A: Implement Certificates and Certificate Authorities
* Topic 6B: Implement PKI Management

**Day 4:**

**Chapter 7: Implementing Authentication Controls**

* Topic 7A: Summarize Authentication Design Concepts
* Topic 7B: Implement Knowledge Based Authentication
* Topic 7C: Implement Authentication Technologies
* Topic 7D: Summarize Biometrics Authentication Concepts

**Chapter 8: Implementing a Secure Network Architecture**

* Topic 8A: Implement Identity and Account Types
* Topic 8B: Implement Account Policies
* Topic 8C: Implement Authorization Solutions
* Topic 8D: Explain the importance of Personnel Policies

**Day 5:**

**Chapter 9: Implementing Secure Network Designs**

* Topic 9A: Implement Secure Network Design
* Topic 9B: Implement Secure Switching and Routing
* Topic 9C: Implement Secure Wireless Infrastructure
* Topic 9D: Implements Load Balancers

**Chapter 10: Implementing Network Security Appliances**

* Topic 10A: Implement Firewalls and Proxy Servers
* Topic 10B: Implement Network Security Monitoring
* Topic 10C: Summarize the Use of SIEM

**Day 6:**

**Chapter 11:** **Implementing Secure Network Protocols**

* Topic 11A: Implement Secure Network Operations Protocols
* Topic 11B: Implement Secure Application Protocols
* Topic 11C: Implement Secure Remote Access Protocols

**Chapter 12: Implementing Host Security Solutions**

* Topic 12A: Implement Secure Firmware
* Topic 12B: Implement Endpoint Security
* Topic 12C: Explain Embedded System Security Implications

**Day 7:**

**Lesson 13: Implementing Secure Mobile Solutions**

* Topic 13A: Implementing Mobile Device Management
* Topic 13B: Implement Secure Mobile Device Connections

**Lesson 14: Summarizing Secure Application Concepts**

* Topic 14A: Analyze Indicators of Application Attacks
* Topic 14B: Analyze Indicators of Web Application Attacks
* Topic 14C: Summarize Secure Coding Practices
* Topic 14D: Implement Secure Script Environments
* Topic 14E: Summarize Deployment and Automation Concepts

**Lesson 15: Implementing Secure Cloud Solution**

* Topic 15A: Summarize Secure Cloud and Virtualization Services
* Topic 15B: Apply Cloud Security Solutions
* Topic 15C: Summarize Infrastructure as Code Concepts

**Day 8:**

**Lesson 16: Explaining Data Privacy and Protection Concepts**

* Topic 16A: Explain Privacy and Data Sensitivity Concepts
* Topic 16B: Explain Privacy and Data Protection Controls

**Lesson 17: Performing Incident Response**

* Topic 17A: Summarize Incident Response Procedures
* Topic 17B: Utilize Appropriate Data Sources For Incident Response
* Topic 17C: Apply Mitigation Controls

**Lesson 18: Explaining Digital Forensics**

* Topic 18A: Explain Key Aspects for Digital Forensics Documentation
* Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

**Day 9:**

**Lesson 19: Summarizing Risk Management Concepts**

* Topic 19A: Explain Risk Management Processes and Concepts
* Topic 19B: Explain Business Impact Analysis Concepts

**Lesson 20: Implementing Cybersecurity Resilience**

* Topic 20A: Implement Redundancy Strategies
* Topic 20B: Implement Backup Strategies
* Topic 20C: Implement Cybersecurity Resilience Strategies

**Lesson 21: Explaining Physical Security**

* Topic 21A: Explain the Importance of Physical Site Security Controls
* Topic 21B: Explain the Importance of Physical Host Security Controls

**Day 10:**

• Overall Course Review

* + PBQs CertMaster Learn - Review
  + CertMaster Practice Exam - Review
  + Labs – Review

• ACE Assessment administered (1-hour timed assessment) last day of class only

* Assessment Review: If the assessment score is lower than 70% after the initial assessment review the student will have the option to retake the assessment

• Evaluation Time: Students will be given 20 minutes to access and complete the evaluation for the class

• To be eligible for exam voucher submit CertMaster Practice Exam to Mentor with 85% and above score (after class completion or graduation)

##### Grading

Grading will be assigned as follows:

* For students to successfully complete the course, they must meet the course participation/attendance and homework completion requirements. Additionally, students seeking an ACE credit recommendation must score a 70 percent or higher on the final assessment.

### Certified Ethical Hacker (CEH)

course DESCRIPTION

This subject will immerse you into an interactive environment where you will be shown how to scan, test, hack and secure your own systems. The lab intensive environment gives you in-depth knowledge and practical experience with the current essential security systems. You will begin by understanding how perimeter defenses work and then be led into scanning and attacking your own networks, no real network is harmed. You will then learn how intruders escalate privileges and what steps can be taken to secure a system. You will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When you leave this intensive 5-day class, you will have hands on understanding and experience in Ethical Hacking.

course OBJECTIVES

* Students will learn:
* Background of technology and technological operations
* Risk and system analysis
* Systems securities and vulnerabilities
* Regulations and ethics

Targeted Job Roles

* Site Administrators
* Security Auditors
* Security Professionals

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* Basic IP addressing knowledge

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| CEH | Certified Ethical Hacker | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

EC-Council Digital Courseware

CEHv9 e-Courseware

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

**Lesson 1: Introduction to Ethical Hacking**

* Information Security Overview
* Information Security Threats and Attack Vectors
* Hacking Concepts, Types, and Phases
* Ethical Concepts Hacking and Scopes
* Information Security Controls
* Physical Security
* Information Management
* Vulnerability Assessment
* Penetration Testing
* Security Laws and Standards

**Lesson 2: Footprinting and Reconnaissance**

* Footprinting Concepts
* Footprinting Methodology
* Footprinting Using Advanced Google Hacking Techniques
* Footprinting Tools
* Footprinting Countermeasures
* Footprinting Penetration Testing

**Lesson 3: Scanning Networks**

* Overview of Network Scanning
* CEH Scanning Methodology

**Lesson 4: Enumeration**

* Enumeration Concepts
* Enumerations Countermeasures
* Enumeration Penetration Testing

**Lesson 5: System Hacking**

* System Hacking: Goals
* CEH Hacking: Methodology
* CEH System Hacking Steps
* Escalating Privileges
* Executing Applications
* Spyware
* Defending Against Keyloggers
* Hiding Files
* Detecting Rootkits
* NTFS Data Stream
* Steganography/Steganlysis
* Covering Tracks

**Lesson 6: Malware Threats**

* Trojan Concepts
* Types of Trojans
* Virus and Worm Concepts
* Ransomware
* Malware Reverse Engineering
* Malware Detection
* Countermeasures
* Penetration Testing

**Lesson 7: Sniffing**

* Sniffing Concepts
* MAC/DHCP Attacks
* IDRP Spoofing
* ARP/DNS Poisoning
* Sniffing Tools
* Detection Techniques
* Counter Measures

**Lesson 8: Social Engineering**

* Social Engineering Concepts
* Social Engineering Techniques
* Identity Theft
* Social Engineering Countermeasures

**Lesson 9: Denial of Service**

* DoS/DDoS Concepts
* DoS/DDoS Attack Techniques
* Botnets
* DoS/DDos Attack Tools
* Counter Measures
* DoS/DDos Protection Tools

**Lesson 10: Session Hijacking**

* Session Hijacking Concepts
* Application Level Hijacking
* Network Level Hijacking
* Hijacking Tools
* Countermeasures

**Lesson 11: Hacking Web Servers**

* Webserver Concepts
* Webserver Attakcs
* Attack Methodology
* Webserver Attack Tools
* Patch Management
* Webserver Security Tools

**Lesson 12: Hacking Web Applications**

* Web App Concepts
* Web App Threats
* Web App Hacking Methodology
* Attack Web Servers
* Analyze Web Apps
* Authorization Attack Schemes
* Perform Injection Attacks
* Attack Data Connectivity

**Lesson 13: SQL Injection**

* SQL Injection Concepts
* Types of SQL Injection
* SQL Injection Methodology
* SQL Injection Tools
* Evasion Techniques
* Counter Measures
* Snort Rule Detection to SQL Injection Attacks
* Detection Tools

**Lesson 14: Hacking Wireless Networks**

* Wireless Statistics
* Wireless Concepts
* Wireless Encryption
* Breaking Encryption
* Defending Against WPA Cracking
* Wireless Threats
* Wireless Hacking Methodology
* WEP/WPA Cracking Tools
* Counter Measures
* Security Tools

**Lesson 15: Hacking Mobile Platforms**

* Mobile Platform Attack Vectors
* Hacking Android/IOS
* Hacking Windows/BlackBerry
* Mobile Device Management
* Mobile Security Guidelines and Tools

**Lesson 16: Evading IDS, Firewalls and Honeypots**

* IDS, Firewall and Honeypot Concepts
* IDS, Firewall and Honeypot Systems
* IDS/Firewall Evading Tools
* Detecting Honeypots
* Counter Measures

**Lesson 17: Cloud Computing**

* Introduction to Cloud Computing
* Cloud Computing Threats/Attacks
* Cloud Security
* Cloud Penetration Testing

**Lesson 18: Cryptography**

* Cryptography Concepts
* Encryption Algorithms
* Cryptography Tools
* Public Key Infrastructure
* Email Encryption
* Disk Encryption
* Cryptography Attacks
* Cryptanalysis Tools

GRADING

Grading will be assigned as follows:

* Attendance: 50%
* Participation: 50%

#### computer hacking forensic investigator (CHFI)

course DESCRIPTION

The Computer Hacking Forensic Investigator program presents a detailed methodological approach to computer forensics and evidence analysis. It is a comprehensive course covering major forensic investigation scenarios that enable students to acquire hands-on experience on various forensic investigation techniques and standard tools necessary to successfully carry out a computer forensic investigation.

If you or your organization requires the knowledge or skills to identify, track, and prosecute the cybercriminals, then this is the course for you. This course helps students to excel in digital evidence acquisition, handling and analysis in a forensically sound manner. Acceptable in a court of law, these skills will lead to successful prosecutions in various types of security incidents such as data breaches, corporate espionage, insider threats and other intricate cases involving computer systems.

CHFI is a certification that gives a complete overview of the process that a forensic investigator must follow when investigating a cybercrime. It includes not only the right treatment of the digital evidence in order to be accepted in the Courts but also useful tools and techniques that can be applied to investigate an incident.

course OBJECTIVES

Students will learn:

* The computer forensic investigation process and the various legal issues involved
* Evidence searching, seizing and acquisition methodologies in a legal and forensically sound manner
* Different types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category
* Roles of first responder, first responder toolkit, securing and evaluating electronic crime scene, conducting preliminary interviews, documenting electronic crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, and reporting the crime scene
* How to set up a computer forensics lab and the tools involved in the lab
* Various file systems and how to boot a disk
* Gathering volatile and nonvolatile information from Windows
* Data acquisition and duplication rules, validation methods and tools required
* How to recover deleted files and deleted partitions in Windows, Mac OS X, and Linux
* The process involved in forensic investigation using AccessData FTK and EnCase
* Steganography and its techniques, Steganalysis, and image file forensics
* Password Cracking Concepts, tools, types of password attacks and how to investigate password protected files
* Different types of log capturing, log management, time synchronization, and log capturing tools
* How to investigate logs, network traffic, wireless attacks, and web attacks
* How to track e-mails and investigate e-mail crimes
* Mobile forensics and mobile forensics software and hardware tools
* How to write investigative reports

Targeted Job Roles

* Junior Computer Forensics Investigator
* Incident Response Technician
* Junior Computer Security Analyst

Admission Requirements

* Individuals applying for this program are required to:
* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* Basic IP addressing knowledge
* Certified Ethical Hacker (CEH) certification or equivalent experience

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| CHFI | Computer Hacking Forensic Investigator | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for night students.

REQUIRED TEXTBOOK

EC-Council Digital Courseware

CHFI v9 e-Courseware

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

Lesson: 1

* Computer Forensics in Today’s World
* Computer Forensics Investigation Process
* Understanding Hard Discs and File Systems

Lesson: 2

* Operating Systems Forensics
* Defeating Anti-Forensic Techniques
* Data Acquisition and Duplication

Lesson: 3

* Network Forensics
* Investigating Web Attacks
* Database Forensics

Lesson: 4

* Cloud Forensics
* Malware Forensics
* Investigating Email Crimes

Lesson: 5

* Mobile Forensics
* Investigative Reports

GRADING

Grading will be assigned as follows:

* Attendance: 50%
* Participation: 50%

CompTIA security +

PROGRAM DESCRIPTION

CompTIA® Security+® (SY0-601) is the primary course you will need to take if your job responsibilities include securing network services, operations and Incident response, governance, Risk and compliance, protecting against attacks, threats and vulnerabilities in your organization. This course prepares you for the CompTIA Security+ certification. In this course, you will build on your knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network. This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (SY0-601) certification, this course can be a significant part of your preparation. However, certification is not the only key to professional success in the field of computer security. 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.

PERFORMANCE OBJECTIVES

##### Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab

##### Course Objectives

Upon completion of this course, students will be able to:

* Identify the fundamental components of information security
* Analyze risk.
* Identify various threats to information security.
* Conduct security assessments to detect vulnerabilities.
* Implement security for hosts and software.
* Implement security for networks.
* Manage identity and access.
* Implement cryptographic solutions in the organization.
* Implement security at the operational level.
* Address security incidents.
* Ensure the continuity of business operations in the event of an incident.

Targeted Job Roles

* IT Security Professionals

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* CompTIA A+ Certification is helpful but not required
* a fundamental understanding of computer and networking concepts
* six to nine months of helpdesk experience recommended

Class Schedule

Day students will attend weekday classes from 8:00AM to 5:00PM for five days. Classes for evening students will be held Monday through Friday from 6:00 PM to 10:00 PM. For day students, a half hour lunch break will be taken every day from 12:00PM to 12:30PM with four 10 minute breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

Tuition and Labs

Registration: $0  
Base Tuition: $2,513  
Labs: $182  
Total Tuition Fee: $2,695

program hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| SY0-601 | CompTIA Security + | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

CompTIA Security+ SYO-601

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 11/12/2020

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM OUTLINE

**Day 1:**

**Chapter 1:** **Comparing Security Roles and Security Controls**

* Topic 1A: Compare and Contrast Information Security Roles
* Topic 1B: Compare and Contrast Security Control and Framework Types

**Chapter 2:**  **Explaining Threat Actors and Threat Intelligence**

* Topic 2A: Explain Threat Actor Types and Attack Vectors
* Topic 2B: Explain Threat Intelligence Sources**Understanding attacks**

**Day 2:**

**Chapter 3: Performing Security Assessments**

* Topic 3A: Assess Organizational Security with Network Reconnaissance Tools
* Topic 3B: Explain Security Concerns with General Vulnerability Types
* Topic 3C: Summarize Vulnerability Scanning Techniques
* Topic 3D: Explain Penetration Testing Concepts

**Chapter 4:** **Identifying Social Engineering and Malware**

* Topic 4A: Compare and Contrast Social Engineering Techniques
* Topic 4B: Analyze Indicators of Malware-Based Attacks

**Day 3:**

**Chapter 5:** **Summarizing Basic Cyptographic Ciphers**

* Topic 5A: Compare and Contrast Basic Cyptographic Ciphers o
* Topic 5B: Summarize Cryptographic Modes of Operation
* Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
* Topic 5D: Summarize Other Cryptographic Technologies

**Chapter 6:** **Implementing Public Key Infrastructure**

* Topic 6A: Implement Certificates and Certificate Authorities
* Topic 6B: Implement PKI Management

**Day 4:**

**Chapter 7: Implementing Authentication Controls**

* Topic 7A: Summarize Authentication Design Concepts
* Topic 7B: Implement Knowledge Based Authentication
* Topic 7C: Implement Authentication Technologies
* Topic 7D: Summarize Biometrics Authentication Concepts

**Chapter 8: Implementing a Secure Network Architecture**

* Topic 8A: Implement Identity and Account Types
* Topic 8B: Implement Account Policies
* Topic 8C: Implement Authorization Solutions
* Topic 8D: Explain the importance of Personnel Policies

**Day 5:**

**Chapter 9: Implementing Secure Network Designs**

* Topic 9A: Implement Secure Network Design
* Topic 9B: Implement Secure Switching and Routing
* Topic 9C: Implement Secure Wireless Infrastructure
* Topic 9D: Implements Load Balancers

**Chapter 10: Implementing Network Security Appliances**

* Topic 10A: Implement Firewalls and Proxy Servers
* Topic 10B: Implement Network Security Monitoring
* Topic 10C: Summarize the Use of SIEM

**Day 6:**

**Chapter 11:** **Implementing Secure Network Protocols**

* Topic 11A: Implement Secure Network Operations Protocols
* Topic 11B: Implement Secure Application Protocols
* Topic 11C: Implement Secure Remote Access Protocols

**Chapter 12: Implementing Host Security Solutions**

* Topic 12A: Implement Secure Firmware
* Topic 12B: Implement Endpoint Security
* Topic 12C: Explain Embedded System Security Implications

**Day 7:**

**Lesson 13: Implementing Secure Mobile Solutions**

* Topic 13A: Implementing Mobile Device Management
* Topic 13B: Implement Secure Mobile Device Connections

**Lesson 14: Summarizing Secure Application Concepts**

* Topic 14A: Analyze Indicators of Application Attacks
* Topic 14B: Analyze Indicators of Web Application Attacks
* Topic 14C: Summarize Secure Coding Practices
* Topic 14D: Implement Secure Script Environments
* Topic 14E: Summarize Deployment and Automation Concepts

**Lesson 15: Implementing Secure Cloud Solution**

* Topic 15A: Summarize Secure Cloud and Virtualization Services
* Topic 15B: Apply Cloud Security Solutions
* Topic 15C: Summarize Infrastructure as Code Concepts

**Day 8:**

**Lesson 16: Explaining Data Privacy and Protection Concepts**

* Topic 16A: Explain Privacy and Data Sensitivity Concepts
* Topic 16B: Explain Privacy and Data Protection Controls

**Lesson 17: Performing Incident Response**

* Topic 17A: Summarize Incident Response Procedures
* Topic 17B: Utilize Appropriate Data Sources For Incident Response
* Topic 17C: Apply Mitigation Controls

**Lesson 18: Explaining Digital Forensics**

* Topic 18A: Explain Key Aspects for Digital Forensics Documentation
* Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

**Day 9:**

**Lesson 19: Summarizing Risk Management Concepts**

* Topic 19A: Explain Risk Management Processes and Concepts
* Topic 19B: Explain Business Impact Analysis Concepts

**Lesson 20: Implementing Cybersecurity Resilience**

* Topic 20A: Implement Redundancy Strategies
* Topic 20B: Implement Backup Strategies
* Topic 20C: Implement Cybersecurity Resilience Strategies

**Lesson 21: Explaining Physical Security**

* Topic 21A: Explain the Importance of Physical Site Security Controls
* Topic 21B: Explain the Importance of Physical Host Security Controls

**Day 10:**

• Overall Course Review

* + PBQs CertMaster Learn - Review
  + CertMaster Practice Exam - Review
  + Labs – Review

• ACE Assessment administered (1-hour timed assessment) last day of class only

* Assessment Review: If the assessment score is lower than 70% after the initial assessment review the student will have the option to retake the assessment

• Evaluation Time: Students will be given 20 minutes to access and complete the evaluation for the class

• To be eligible for exam voucher submit CertMaster Practice Exam to Mentor with 85% and above score (after class completion or graduation)

##### Grading

Grading will be assigned as follows:

* For students to successfully complete the course, they must meet the course participation/attendance and homework completion requirements. Additionally, students seeking an ACE credit recommendation must score a 70 percent or higher on the final assessment.

## IT Project Management Professional - CAPM/PMP

### Program Description

This program is based on the Project Management Professional (PMP) and Service Management (ITIL) credentials. The PMP is one of the most important industry-recognized certification for IT project managers. Globally recognized and demanded, the PMP demonstrates that students have the experience, education and competency to lead and direct projects. This recognition is seen through increased marketability to employers and higher salary; according to the PMI Project Management Salary Survey–Seventh Edition, this certification positively impacts project manager salaries.

Our PMP program has a strong IT orientation and covers a number of foundational IT management skills in addition to the core project management skills. The program introduces the principles and core elements of project management and IT service management (ITSM) based on ITIL framework, then moves into advanced project management principles including topics that prepare the student for the PMP certification.

### Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| ITIL | ITIL Foundations | 24/16/0/40 |
| CAPM/PMP | PMP Exam Preparation | 40/0/0/40 |

The approximate time required to complete this program is ten days for day students and twenty days for evening students.

Class Schedule

Day students will attend weekday classes from 8:00AM to 5:00PM for five days. Classes for evening students will be held Monday through Friday from 7:00 PM to 11:00PM. For day students, an hour lunch break will be taken every day from 11:30AM to 12:30PM with four 10 minute breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

### Tuition and Fees

Registration: $0  
Tuition: $5,399  
Labs: $191  
Total Tuition Fee: $5,590

### Targeted Job Roles

* Project Manager
* Business Analyst
* Service Delivery Manager
* Incident Manager
* Engagement Manager
* Client Service Manager
* Technical Support Manager
* Software Engineering Manager
* QA Analyst

### Subject Descriptions

#### ITIL v4 foundations

course DESCRIPTION

Based on the ITIL best practice service lifecycle approach, this course provides IT managers, practitioners and anyone who uses IT services with a practical understanding of the key concepts, principles, processes, and functions that enables successful IT Service Management (ITSM) provision. The course intent is to provide proven practical guidance on how to successfully introduce an integrated IT Service Management framework and how best practices can be adopted and adapted within an organization. It also prepares students for the ITIL Foundation Certificate. This is for IT project managers and practitioners involved in the strategy, design, implementation and on-going delivery of business-used IT services and for anyone who requires an insight into Service Management best practice.

course OBJECTIVES

Students will learn:

* Key concepts of ITIL
* Important principles for improving IT operations and project success
* Vital processes and functions
* Practical guidance for applying ITIL to everyday IT project situations
* How to align with business, control costs, and improve IT service quality
* Strategies to balance IT resources

Targeted Job Roles

* IT Professionals with an interest in Service Management

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| ITL-FND | ITIL v4 Foundations | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

ITIL 4 Foundation

Course Developer: Logical Operations

Authors: Patrick Von Schlag ITIL Expert

Laurie Perry

Publish Date2019

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

**Day 1**

Module 1: Introduction

* Introduction/Housekeeping
* Introduction to key ITIL concepts
* IT as a Service
* Introduction to processes and process management
* The Service Lifecycle approach

Module 2: Service Strategy

* Purpose, goal, objectives & Scope
* Value Creation through Services
* Assets - Resources and Capabilities
* Service Strategy - Main activities
* Service Strategy processes
* Service Portfolio management
* Demand management
* Financial management
* Business Relationship Management

**Day 2**

Module 3: Service Design

* Purpose, goal, objectives & Scope
* Service Design processes
* The 4 P's
* Service Design aspects
* Service Catalog Management
* Service Level Management
* Capacity Management
* Availability Management
* IT Service Continuity Management
* Service Portfolio
* Information Security Management
* Supplier management
* Design Coordination

Module 4: Service Transition

* Purpose, goal, objectives & Scope
* Service Transition value to the business
* Technology and architecture in Service Transition
* Service Transition Processes
* Change Management
* The 7 R's of Change Management
* Service Asset and Configuration Management
* Release and Deployment Management
* Knowledge Management

**Day 3**

Module 5: Service Operation

* Purpose, goal, objectives & Scope
* Service Operation definitions
* The Service Desk
* Technical Management
* Application Management
* IT Operations Management
* Service Operations Processes
* Event Management
* Request Fulfillment
* Problem Management
* Access Management

Module 6: Continual Service Improvement

* Purpose, goal, objectives & Scope
* Models and Processes
* The Deming Cycle
* Measurement and metrics
* Continual Service Improvement activities
* Risk management
* Continual Service Improvement interfaces
* Interface with Service Level Management

#### capm/PMP: PMP Preparation

course DESCRIPTION

You can find PMPs leading projects in nearly every country and, unlike other certifications that focus on a particular geography or domain, the PMP® is truly global. As a PMP, you can work in virtually any industry, with any methodology and in any location. The PMP signifies that you speak and understand the global language of project management and connects you to a community of professionals, organizations and experts worldwide.

This course provides an intensive review of the subject matter tested on the Project Management Institute’s Project Management Professional (PMP) certification. This course will provide a summary review of the nine knowledge areas and five process groups covered in A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Participants will improve their test-taking skills by completing sample test totaling 200 questions and by discussing the rationale behind both correct and incorrect answers. The program is specifically designed to maximize the probability that you will succeed in passing the PMP certification the first time. Each student will receive a student manual including review materials, key definitions and formulas, sample questions and answers.

PERFORMANCE OBJECTIVES

Students will learn:

* Initiating Domains.
* Planning Domains.
* Executing Domains.
* Monitoring Domains.
* Closing Domains.

Targeted Job Roles

* Project Managers

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills

course hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| PMP-EP | Project Management Professional | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

Project Management Institute

PMBOK 6h Edition

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

course OUTLINE

**Lesson 1:**

Module 1: Project Management Fundamentals

* Key Project Management Definitions
* Role of the Project Manager
* Knowledge Areas and Process Groups
* Project Lifecycle Models
* Project Processes
* Organizational Influences on Project Management
* Project Maturity Models

Module 2: Project Initiation

* Project Selection Process
* Project Charter Elements
* Exercise 1: Prepare Project Charter and Milestone Schedule
* Stakeholder Identification
* Exercise 2: Identify Stakeholders

Module 3: Planning the Project

* Project Requirements
* Class Exercise: Define Case Study Requirements
* Scope Definition & Management
* Work Breakdown Structure
* Exercise 3: Prepare WBS
* Schedule Development
* Define Activities
* Sequence Activities
* Estimate Durations
* Develop Schedule
* Exercise 4: Prepare Project Schedule using Critical Path Method

**Lesson 2:**

Module 3: Planning the Project (continued)

* Cost Estimating and Budgeting
* Project Risk Management
* Risk Identification
* Risk Analysis
* Risk Response Planning
* Exercise 5: Prepare Risk Management Plan
* Project Communications
* Managing Expectations
* Stakeholder Communications
* Assigning Responsibilities using a RACI Chart
* Exercise 6: Prepare RACI Chart & Communications Plan

Module 4: Executing, Monitoring and Controlling the Project

* Integrated Change Control
* Exercise 7: Decide on Change Order Resolution
* Risk Monitoring and Control
* Exercise 8: Manage Risk Event

Module 5: Project Close-out

* Project Closing and Acceptance
* Project Archives and Lessons Learned

Course Wrap-up

* Review of Key Learning's & How to Apply to Projects

**Lesson 3:**

Module 6: Introduction and PMP® Program Overview

* Applying for and Taking the Exam
* Strategies: General and Question-by-Question

Module 7: Project Management Framework

* Project Life Cycles and Stakeholder Management
* The Triple Constraint and Organizational Issues

Module 8: Project Scope Management

* Initiating the Project: Project Plans
* Work Breakdown Structures

**Lesson 4:**

Module 9: Project Time Management

* Project Schedules and Logic Diagramming
* Critical Path Analysis and Performance Measurement

Module 10: Project Human Resource Management

* Project Manager Responsibilities
* Power & Conflict Management

Module 11: Project Quality Management

* Project Management and Quality management
* Statistical Process Control

Module 12: Project Cost Management

* Estimating versus Pricing
* Financial Analysis

**Lesson 5:**

Module 13: Project Procurement Management

* Procurement Planning
* Business Issues, Selection, and Evaluation

Module 14: Project Risk Management

* Expected Values
* Decision Trees and Cause and Effect

Module 15: Project Communication Management

* Tools and Techniques
* Reporting and Lessons Learned

Module 16: Professional Responsibility

* Professional Responsibility
* Ethics

GRADING

Grading will be assigned as follows:

* Attendance: 75%
* Participation: 25%

CompTIA Network +

PROGRAM DESCRIPTION

The *CompTIA® Network+®* course builds on your existing user-level knowledge and experience with personal computer operating systems and networks to present the fundamental skills and concepts that you will need to use on the job in any type of networking career. If you are pursuing a CompTIA technical certification path, the CompTIA A+ certification is an excellent first step to take before preparing for the CompTIA Network+ certification.

 Also, if your job duties include network troubleshooting, installation, or maintenance, or if you are preparing for any type of network-related career, it provides the background knowledge and skills you will require to be successful.

program OBJECTIVES

Students will learn:

* Identify basic network theory concepts and major network communications methods.
* Describe bounded network media.
* Identify unbounded network media.
* Identify the major types of network implementations.
* Identify TCP/IP addressing and data delivery methods.
* Implement routing technologies.
* Identify the major services deployed on TCP/IP networks.
* Identify the infrastructure of a WAN implementation.
* Identify the components used in cloud computing and virtualization.
* Describe basic concepts related to network security.
* Prevent security breaches.
* Respond to security incidents.
* Identify the components of a remote network implementation.
* Identify the tools, methods, and techniques used in managing a network.
* Describe troubleshooting of issues on a network.

Targeted Job Roles

* Entry-level IT Professional

Admission Requirements

Individuals applying for this program are required to:

* Interview with a Career Training Consultant
* Be at least 18 years of age
* Present proof of secondary education (high school diploma or GED certificate)
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score of 17 on the Wonderlic Scholastic Level Exam.

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* Professional Helpdesk or Computer Support Experience
* CompTIA A+ Certification is helpful but not required

Tuition and Fees

Registration: $0  
Tuition: $2,713  
Labs: $182  
Total Tuition Fee: $2,895

Class Schedule

Day students will attend weekday classes from 8:00AM to 5:00PM for five days. Classes for evening students will be held Monday through Friday from 7:00 PM to 11:00PM. For day students, an hour lunch break will be taken every day from 11:30AM to 12:30PM with four 10 minute breaks dispersed throughout the day. For evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

program hours

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Contact Hours** |
| N10-007 | CompTIA Network + | 40 |

The approximate time required to complete this program is five days for day students, and approximately 10 nights for evening students.

REQUIRED TEXTBOOK

CompTIA Network+ N10-007

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 3/3/20

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

|  |  |
| --- | --- |
| Lab Time | 20 hours |
| Lecture Time | 20 hours |

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM OUTLINE

**Day 1:**

**Chapter 1: Fundamentals**

* Module A: Networking concepts
* Module B: Classifying networks
* Module C: Network models
* Module D: The troubleshooting process

**Chapter 2: Physical networks**

* Module A: Connection technologies
* Module B: Network devices
* Module C: Copper media
* Module D: Optical media
* Module E: Ethernet standards

**Day 2:**

**Chapter 3: TCP/IP networks**

* Module A: IP addressing
* Module B: Core protocols
* Module C: Network ports and applications

**Chapter 4: Internetworking**

* Module A: Switching
* Module B: Routing

**Chapter 5: Wireless LANs**

* Module A: Wireless networks
* Module B: Wireless LAN standards

**Day 3:**

**Chapter 6: Wide area networks**

* Module A: Internet connections
* Module B: WAN infrastructure

**Chapter 7: Cybersecurity principles**

* Module A: Goals and threats
* Module B: Digital security
* Module C: Transport encryption

**Day 4:**

**Chapter 8: Defending networks**

* Module A: Network security components
* Module B: Network authentication systems
* Module C: Hardening networks

**Chapter 9: Evolving network technologies**

* Module A: Network convergence
* Module B: Virtual and cloud systems

**Day 5:**

**Chapter 10: Network operations**

* Module A: Monitoring and optimization
* Module B: Fault tolerance and disaster recovery
* Module C: Incident response

**Chapter 11: Network planning**

* Module A: Network policy design
* Module B: Network installation
* Module C: Maintenance and upgrades

GRADING

Grading will be assigned as follows:

* Attendance: 50%
* Participation: 50%

“The information contained in this catalog is true and correct to the best of my knowledge.”

Meghan Jurado, Compliance Manager

Signature: Meghan Jurado, 2/18/21

1. More simply, the refund is based on the precise number of course time hours the student has paid for, but not yet used, at the point of termination, up to the 75% completion mark, after which no refund is due. Form PS-1040R provides the precise calculation. [↑](#footnote-ref-1)