

ACI Learning

102 Decker Court, Suite 250

Irving, Texas 75062

Phone: (972) 865-4030

Toll Free: (866) 378-0761

Fax: (303) 768-0513

Catalog Number 1, Volume Number 20, Revised 1/26/2021

Effective Date 1/26/2021

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

Table of Contents

[Introduction 4](#_Toc62636513)

[Administration Staff 4](#_Toc62636514)

[Faculty 5](#_Toc62636515)

[Programs Offered 5](#_Toc62636516)

[Tuition and LABS 7](#_Toc62636517)

[Class Schedule 8](#_Toc62636518)

[Full time Students: 8](#_Toc62636519)

[Part-Time Students: 8](#_Toc62636520)

[Entrance Requirements 9](#_Toc62636521)

[Enrollment 9](#_Toc62636522)

[Facilities 9](#_Toc62636523)

[Placement Assistance 12](#_Toc62636524)

[Attendance Requirements 12](#_Toc62636525)

[VA Benefit Disbursement DELAYS 13](#_Toc62636526)

[Certification Policy 14](#_Toc62636527)

[Grading System/Progress Reports 14](#_Toc62636528)

[ACE Credit ASSESSMENT 15](#_Toc62636529)

[aci Virtual live offerings- HYBRID 15](#_Toc62636530)

[Re-Admission Policy 16](#_Toc62636531)

[Graduation Policy 16](#_Toc62636532)

[Reschedule Policy 16](#_Toc62636533)

[Cancellation and Refund Policy 16](#_Toc62636534)

[Conduct Policy 18](#_Toc62636535)

[Student Complaints 18](#_Toc62636536)

[Educational Services 18](#_Toc62636537)

[Previous Credits 19](#_Toc62636538)

[Dismissal 19](#_Toc62636539)

[Student Grievance Procedure 19](#_Toc62636540)

[Programs 20](#_Toc62636541)

[Technical Support Specialist Classroom (TSS) 20](#_Toc62636542)

[TECHINCAL SUPPORT SPECIALIST HYBRID 20](#_Toc62636543)

[Computer User Support Specialist classroom (CUSS) 32](#_Toc62636544)

[COMPUTER USER SUPPORT SPECIALIST HYBRID 32](#_Toc62636545)

[Network Supp0ort Specialist CLASSROOM (NSS) 51](#_Toc62636546)

[NETWORK SUPPORT SPECIALIST HYBRID 51](#_Toc62636547)

[CCNA CLASSROOM 65](#_Toc62636548)

[CCNA HYBRID 65](#_Toc62636549)

[Information Security Analyst Classroom (ISA) 72](#_Toc62636550)

[INFORMATION SECURITY ANALYST Hybrid 72](#_Toc62636551)

[Cybersecurity Specialist CLASSROOM (CYBER) 85](#_Toc62636552)

[CYBERSECURITY SPECIALIST HYBRID 85](#_Toc62636553)

[CompTIA security + CLASSROOM 97](#_Toc62636554)

[cOMPTIA SECURITY + HYBRID 97](#_Toc62636555)

[IT Project Management Professional CLASSROOM 101](#_Toc62636556)

[IT PROJECT MANAGEMENT PROFESSIONAL HYBRID 101](#_Toc62636557)

[CompTIA Network + 109](#_Toc62636558)

[EC-Council Computer Hacking Forensic Investigator (CHFI) 113](#_Toc62636559)

[Certified Ethical Hacker Training (CEH) 116](#_Toc62636560)

[Certified Network Defender (CND) 121](#_Toc62636561)

[CompTIA Advanced Security Practitioner (CASP) 124](#_Toc62636562)

[CAPM/PMP- IT Project Manager 127](#_Toc62636563)

[ITIL v3 Foundations 132](#_Toc62636564)

[Certified Information Systems Security Professional Training (CISSP) 135](#_Toc62636565)

[AWS re/Start Cloud Support CLASSROOM (AWS) 139](#_Toc62636566)

[AWS RE/START CLOUD SUPPORT HYBRID 139](#_Toc62636567)

# 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 five 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 ACI Learning 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: Texas approved for GI BILL ® Benefits
* June 2018: ACI Learning San Antonio is approved by TWC.
* May 2019 ACI Learning is acquired by MISTI, all staff and programs retained.
* 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
* Bob Villareal – Campus Director – Irving
* David Koker- Campus Director- San Antonio
* Qwincy Houston – Campus Director – Denver
* Chris Young – Campus Director – Colorado Springs
* Jennifer Mathis – Campus Director – Jacksonville
* Meghan Jurado –Director of Compliance/Lead SCO
* Mary Walker – Accounting

Dallas Staff:

* Bob Villareal – Campus Director – Dallas
* George Clay – Sr Career Training Consultant
* Robert MacIntyre – Career Training Consultant
* Brandon Smith – Career Training Consultant
* Miranda Murphey- Career Training Consultant
* Jay Thompson- Career Training Consultant
* Rod Otis- Lead Instructor
* Jesse Dubose- Employment Engagement Manager
* Eleeta Wesley- Employment Development Manager
* Jan Campo – Test Center Administrator
* Kebria Topps- Frontline Associate

# Faculty

**Rod Oatis –Technical Instructor**

Rod has over 22 years in the IT Technology Industry and is highly invested in teaching other students to be successful in their IT careers.

* CompTIA A+
* CompTIA Network+
* CompTIA Security+
* ITIL Foundations

# 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 Application | 40 |
| Computer User Support Specialist (CUSS) | 220-1001 | A+ Essentials | 40 | 25 |
| 220-1002 | A+ Practical Applications | 40 |
| Net+ | Network+ | 40 |
| Sec+ | 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) | Net+ | Network+ | 40 | 20 |
| Sec+ | 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 | AWS Fundamentals, Cloud & SysOps | 320 | 40 |
| **Information Security** | | | | |
| Information Security Analyst- ISA | Sec + | Security + | 40 | 15 |
| CND | Certified Network Defender Training | 40 |
| CEH | Certified Ethical Hacker Training | 40 |
| Cybersecurity Specialist (CYBER) | Sec+ | Security+ | 40 | 15 |
| CEH | Professional Ethical Hacker Training | 40 |
| CHFI | EC- Council Computer Hacking Forensics Investigator | 40 |
| CompTIA Security + | SYO-601 | Security + | 40 | 5 |
| CompTIA Advanced Security Practitioner | CASP | CompTIA Advanced Security Practitioner | 40 | 5 |
| Certified Digital Forensics Examiner | CHFI | EC-Council Certified Digital Forensics Examiner | 40 | 5 |
| Certified Information Systems Security Professional | CISSP | Certified Information Systems Security Professional Training | 40 | 5 |
| Certified Professional Ethical Hacker | CEH | Certified Ethical Hacker Training | 40 | 5 |
| Certified Network Defender | CND | Certified Network Defender Training | 40 | 5 |
| **Project and Service Management** | | | | |
| IT Project Management Professional | ITIL | ITIL Foundations | 40 | 10 |
| CAPM/PMP | PMP | 40 |
| ITIL Foundations | ITIL | ITIL Foundations | 40 | 5 |
| IT Project Manager | CAPM/PMP | PMP | 40 | 5 |

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

# Tuition and LABS

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Programs** | | | | | | | | | | |
| **Base Tuition** | **Labs** | | | | | | | **Total Tuition** | | |
| 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 + (Sec +) – 40 hours | | | | | | | | | | |
| $2,713 | | | | $182 | | | | | | $2,895 |
|  | | | | | | | | | | |
| EC Council Computer Hacking Forensic Investigator (CHFI) – 40 hours | | | | | | | | | | |
| $3,348 | | | | | $447 | | $3,795 | | | |
|  | | | | | | | | | | |
| CompTIA Advanced Security Practitioner (CASP)- 40 hours | | | | | | | | | | |
| $3, 309 | | | | | $186 | | $3,495 | | | |
|  | | | | | | | | | | |
| Certified Ethical Hacker Training (CEH) – 40 hours | | | | | | | | | | |
| $3,303 | | | | | $492 | | $3,795 | | | |
|  | | | | | | | | | | |
| Certified Network Defender Training (CND) – 40 hours | | | | | | | | | | |
| $3,416 | | | | | $379 | | $3,795 | | | |
|  | | | | | | | | | | |
| CompTIA Network+ (Net+) – 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: [www.acilearning.com](http://www.acilearning.com) 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, equivalency diploma, or a military DD-214 and have a willingness to learn. 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, they must 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, Englewood 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 1000, 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 August 1, 2020:

|  |  |  |  |
| --- | --- | --- | --- |
| **Englewood, CO** | | | |
|  | Address | | 6855 S Havana St, Suite 230, Englewood, CO 80112 |
|  | Total Square Footage | | 6,932 Sq. Ft. |
|  | Number of Classrooms | | 3 |
|  | Student Stations in Classroom #1 | | 12 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #2 | | 16 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #3 | | 12 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 Dr, Suite 250 Colorado Springs, CO 80920 |
|  | Total Square Footage | | 5,049 Sq. Ft. |
|  | Number of Classrooms | | 4 Classrooms |
|  | Student Stations in Classroom #1 | | 18 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #2 | | 18 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #3 | | 20 Dell Optiplex machines with dual monitors |
|  | Student Stations in Classroom #4 | | 24 Dell Optiplex machines with dual monitors |
|  | Lab Environment | | A separate lab room shared between both classrooms |
|  | 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  1 Conference Room  1 Break Area  1 Reception 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 | 20 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. | |
|  |  | |  |
| **San Antonio, TX** | | | |
|  | Address | | 8200 IH-10 West, Suite 1005, San Antonio, TX 78230 |
|  | Total Square Footage | | 2,350 Sq. Ft. |
|  | Number of Classrooms | | 1 Classroom |
|  | Student Stations in Classroom #1 | | 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 |
|  |  | |  |
| **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 |
|  | | | |

# 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 they 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.

# VA Benefit Disbursement DELAYS

Any covered individual wishing to attend classes using their GI BILL ® or VOC Rehab are covered under Title 38 United States Code Section 3679(e). A covered individual isany individual who is entitled to educational assistance under chapter 31, Vocational Rehabilitation and Employment, or chapter 33, Post-9/11 GI Bill ® benefits.

Any covered individual that wishes to attend ACI Learning courses or programs of education during the period beginning on the date on which the individual provides to the educational institution a certificate of eligibility for entitlement to educational assistance under chapter 31 or 33 (a “certificate of eligibility” can also include a “Statement of Benefits” obtained from the Department of Veterans Affairs’ (VA) website – eBenefits, or a VAF 28-1905 form for chapter 31 authorization purposes) and ending on the earlier of the following dates:

1. The date on which payment from VA is made to the institution.
2. 90 days after the date the institution certified tuition and fees following the receipt of the certificate of eligibility.

Delay of disbursement from the VA will not impose any penalty on the covered individual, including the assessment of late fees, the denial of access to classes, libraries, or other institutional facilities, or the requirement that a covered individual borrow additional funds, on any covered individual because of the individual’s inability to meet his or her financial obligations to the institution due to the delayed disbursement funding from VA under chapter 31 or 33.

In order to proceed with the educational requirement prior to receipt of VA disbursement, covered individuals are required to:

1. Submit a certificate of eligibility for entitlement to educational assistance no later than the first day of a course of education.
2. Submit a written request to use such entitlement in the form of a ACI Learning enrollment packet.
3. Provide additional information necessary to the proper certification of enrollment by the educational institution.

If the VA disbursement is paid and there is a shortfall of funds, an additional payment in the amount of the shortfall will need to be made to the school in a timely manner worked out between ACI Learning and the covered individual. This payment will only be equal to the original amount minus the VA disbursement received and no further penalty will be administered.

# 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 Client Services.

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.

# 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.

# 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 ClientServices@ACILearning.com 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.

# 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 (does not apply to Subjects).

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 ALL VA ELIGIBLE PERSON AND THOSE CALLED TO ACTIVE DUTY:

**It is understood and agreed that the following refund policy will be applied to all VA eligible persons:**

In the event that the VA eligible person fails to enter the course, or withdraws, or is discontinued at any time prior to completion of the approved program length for VA students, the amount charged to the student for tuition, fees, and other charges for the completed portion of the course should not exceed $10.00 (only if a registration fee is charged) plus the approximate pro rata portion of the total charges for tuition, fees and other charges that the length of the completed portion of the course bears to its total length. The completed portion is the total number of days the student was scheduled to attend (from first to last date of attendance) multiplied by the scheduled hours of attendance per day.

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 40 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. 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

Attempting to resolve any issue with the School first is strongly encouraged. ACI Learning endeavors to assist students quickly and completely, and requests that students email instructors and Client Services to attempt to solve any issues.

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 [bob.villareal@](mailto:bob.villareal@)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 Classroom (TSS)

## TECHINCAL SUPPORT SPECIALIST HYBRID

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
* 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.

aws

Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| ITIL | ITIL Foundations | 20/20/0/40 |
| A+ 1001 | CompTIA A+ Core 1 | 20/20/0/40 |
| A+ 1002 | CompTIA A+ Core 2 | 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 Labs

Registration: $0  
Base 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 v4 foundations

PROGRAM 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.

##### Subject Hours

40 hours total:

* 40 hours lecture
* 0 hours lab
* 0 hours externship

##### 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

##### Who Should Attend

Anyone seeking ITIL Foundation certification and everyone interested in aligning IT with business, controlling or reducing IT costs, improving IT service quality, and balancing IT resources in the most effective manner. All IT professionals, IT project managers, IT managers, IT project or team members, coordinators, network operators, business process analysts, IT architects, consultants, systems integrators, help desk managers and staff, planners, managed service providers, outsourcers, application developers, and other IT-related positions.

##### Prerequisites

There are no prerequisites for this course.

##### Requird Textbooks

ITIL 4 Foundation

Course Developer: Logical Operations

Authors: Patrick Von Schlag ITIL Expert

Laurie Perry

Publish Date2019

##### Instructional Methods

* Lecture
* Overhead slides

##### Maximum Student to Instructor Ratio

20:1

##### Lesson Plan

**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, 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.

## Computer User Support Specialist classroom (CUSS)

## COMPUTER USER SUPPORT SPECIALIST HYBRID

### 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
* 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.

Modality Versions

Our Computer User Support Specialist is available in two modalities, Computer User Support Specialist Hybrid and Computer User Support Specialist Classroom.

For our Hybrid class version, students will be taught in real-time, with their questions addressed by a live instructor over audio, and in chat over a video meeting. 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.

For our classroom only version, students will be taught on campus with a live instructor with no option to attend virtually.

The content and instruction of both modalities is identical, the only difference is the delivery method.

### 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 |
| Net+ | Network+ | 20/20/0/40 |
| Sec+ | 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 Labs

Registration: $0  
Base 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

##### Subject 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.

##### Subject Hours

40 hours total:

* 24 hours lecture
* 16 hours lab
* 0 hours externship

##### 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

##### Who Should Attend

Anyone seeking ITIL Foundation certification and everyone interested in aligning IT with business, controlling or reducing IT costs, improving IT service quality, and balancing IT resources in the most effective manner. All IT professionals, IT project managers, IT managers, IT project or team members, coordinators, network operators, business process analysts, IT architects, consultants, systems integrators, help desk managers and staff, planners, managed service providers, outsourcers, application developers, and other IT-related positions.

##### Prerequisites

There are no prerequisites for this course.

##### Requird Textbooks

ITIL 4 Foundation

Course Developer: Logical Operations

Authors: Patrick Von Schlag ITIL Expert

Laurie Perry

Publish Date2019

##### Instructional Methods

* Lecture
* Overhead slides

##### Maximum Student to Instructor Ratio

20:1

##### Lesson Plan

**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 Core 1

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+ Core 1 | 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+ 1002- Core 2

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+ Core 2 | 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 +

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.

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
* 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.

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: 30 Bird Media

Author: Clifford J. Coryea, Donald P. Tremblay, Adam A. Wilcox

Publish Date: 2017

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 +

##### Subject 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.

##### 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.

##### Textbooks / Courseware

CompTIA Security+ SYO-601

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 11/12/2020

##### Instructional Methods

* Lecture
* PPT slides
* Labs
* Test Prep
* Written Assignments and Assessments

##### Maximum Student to Instructor Ratio

20:1

##### 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 CLASSROOM (NSS)

## NETWORK SUPPORT SPECIALIST HYBRID

### 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
* 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.

Modality Versions

Our Network Support Specialist is available in two modalities, Network Support Specialist Hybrid and Network Support Specialist Classroom.

For our Hybrid class version, students will be taught in real-time, with their questions addressed by a live instructor over audio, and in chat over a video meeting. 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.

For our classroom only version, students will be taught on campus with a live instructor with no option to attend virtually.

The content and instruction of both modalities is identical, the only difference is the delivery method.

### 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** |
| Net+ | CompTIA Network+ | 20/20/0/40 |
| Sec+ | 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 Labs

Registration: $0  
Base 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.

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
* 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: 30 Bird Media

Author: Clifford J. Coryea, Donald P. Tremblay, Adam A. Wilcox

Publish Date: 2017

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 +

##### Subject 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.

##### 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.

##### Textbooks / Courseware

CompTIA Security+ SYO-601

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 11/12/2020

##### Instructional Methods

* Lecture
* PPT slides
* Labs
* Test Prep
* Written Assignments and Assessments

##### Maximum Student to Instructor Ratio

20:1

##### 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

Program 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.

Prerequisites

Students should have basic computer literacy, and basic Windows navigation, Internet usage, and email usage skills.

Lesson Plan

* 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 CLASSROOM

## CCNA HYBRID

### 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
* 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.

Modality Versions

Our CCNA program is available in two modalities, CCNA Hybrid and CCNA Classroom.

For our Hybrid class version, students will be taught in real-time, with their questions addressed by a live instructor over audio, and in chat over a video meeting. 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.

For our classroom only version, students will be taught on campus with a live instructor with no option to attend virtually.

The content and instruction of both modalities is identical, the only difference is the delivery method.

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| 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 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 Labs

Registration: $0  
Base 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

Program 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.

Prerequisites

Students should have basic computer literacy, and basic Windows navigation, Internet usage, and email usage skills.

Lesson Plan

* 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

## Information Security Analyst Classroom (ISA)

## INFORMATION SECURITY ANALYST Hybrid

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 cyber network defense from three approaches: 1) Preventive 2) Reactive 3) Retrospective.

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
* 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.

Modality Versions

Our Information Security Analyst program is available in two modalities, Information Security Analyst Hybrid and Information Security Analyst Classroom.

For our Hybrid class version, students will be taught in real-time, with their questions addressed by a live instructor over audio, and in chat over a video meeting. 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.

For our classroom only version, students will be taught on campus with a live instructor with no option to attend virtually.

The content and instruction of both modalities is identical, the only difference is the delivery method.

Program Outline

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

Registration: $0  
Base 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 +

##### Subject 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.

##### 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.

##### Textbooks / Courseware

CompTIA Security+ SYO-601

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 11/12/2020

##### Instructional Methods

* Lecture
* PPT slides
* Labs
* Test Prep
* Written Assignments and Assessments

##### Maximum Student to Instructor Ratio

20:1

##### 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 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
* 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

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.

course hours

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

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 Training (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.

PERFORMANCE 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
* 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** |
| 312-50 CEH | Certified Ethical Hacker Training | 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%

## Cybersecurity Specialist CLASSROOM (CYBER)

## CYBERSECURITY SPECIALIST HYBRID

### 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 Wonderlic Basic Skills Test.

Modality Versions

Our CyberSecurity Specialist Program is available in two modalities, CyberSecurity Specialist Hybrid and CyberSecurity Specialist Classroom.

For our Hybrid class version, students will be taught in real-time, with their questions addressed by a live instructor over audio, and in chat over a video meeting. 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.

For our classroom only version, students will be taught on campus with a live instructor with no option to attend virtually.

The content and instruction of both modalities is identical, the only difference is the delivery method.

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| Sec+ | Security+ | 20/20/0/40 |
| CEH | Certified Ethical Hacker Training | 20/20/0/40 |
| CHFI | EC-Council 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 Labs

Registration: $0  
Base Tuition: $9,160  
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 +

##### Subject 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.

##### 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.

##### Textbooks / Courseware

CompTIA Security+ SYO-601

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 11/12/2020

##### Instructional Methods

* Lecture
* PPT slides
* Labs
* Test Prep
* Written Assignments and Assessments

##### Maximum Student to Instructor Ratio

20:1

##### 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 Training (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.

PERFORMANCE 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
* 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** |
| 312-50 CEH | Certified Ethical Hacker Training | 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%

#### EC-Council 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
* 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 | EC-Council 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 + CLASSROOM

cOMPTIA SECURITY + HYBRID

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.

Modality Versions

Our CompTIA Security + Program is available in two modalities, CompTIA Security + Hybrid and CompTIA Security + Classroom.

For our Hybrid class version, students will be taught in real-time, with their questions addressed by a live instructor over audio, and in chat over a video meeting. 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.

For our classroom only version, students will be taught on campus with a live instructor with no option to attend virtually.

The content and instruction of both modalities is identical, the only difference is the delivery method.

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
* 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

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 evening students.

Tuition and Labs

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

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.

## IT Project Management Professional CLASSROOM

## IT PROJECT MANAGEMENT PROFESSIONAL HYBRID

### 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
* 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.

Modality Versions

Our IT Project Management Professional Program is available in two modalities, IT Project Management Professional Hybrid and IT Project Management Professional Classroom.

For our Hybrid class version, students will be taught in real-time, with their questions addressed by a live instructor over audio, and in chat over a video meeting. 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.

For our classroom only version, students will be taught on campus with a live instructor with no option to attend virtually.

The content and instruction of both modalities is identical, the only difference is the delivery method.

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| ITIL | ITIL Foundations | 20/20/0/40 |
| 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 Labs

Registration: $0  
Base 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 v3 foundations

##### Subject 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.

##### Subject Hours

40 hours total:

* 24 hours lecture
* 16 hours lab
* 0 hours externship

##### 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

##### Who Should Attend

Anyone seeking ITIL Foundation certification and everyone interested in aligning IT with business, controlling or reducing IT costs, improving IT service quality, and balancing IT resources in the most effective manner. All IT professionals, IT project managers, IT managers, IT project or team members, coordinators, network operators, business process analysts, IT architects, consultants, systems integrators, help desk managers and staff, planners, managed service providers, outsourcers, application developers, and other IT-related positions.

##### Prerequisites

There are no prerequisites for this course.

##### Requird Textbooks

ITIL 4 Foundation

Course Developer: Logical Operations

Authors: Patrick Von Schlag ITIL Expert

Laurie Perry

Publish Date2019

##### Instructional Methods

* Lecture
* Overhead slides

##### Maximum Student to Instructor Ratio

20:1

##### Lesson Plan

**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%

#### capm/PMP: PMP Exam 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 questions 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 the first time. Each student will receive a student manual including review materials, key definitions and formulas, sample questions and answers.

course 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
* 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

subject 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 5th 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 Certification
* 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.

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
* 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 Labs

Registration: $0  
Base 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: 30 Bird Media

Author: Clifford J. Coryea, Donald P. Tremblay, Adam A. Wilcox

Publish Date: 2017

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%

EC-Council Computer Hacking Forensic Investigator (CHFI)

PROGRAM 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.

program 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
* 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

Tuition and Labs

Registration: $0  
Base Tuition: $3,348  
Labs: $447  
Total Tuition Fee: $3,795

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** |
| CHFI | EC-Council 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

PROGRAM 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%

Certified Ethical Hacker Training (CEH)

PROGRAM 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.

program 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
* 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

Tuition and Labs

Registration: $0  
Base Tuition: $3,303  
Labs: $492   
Total Tuition Fee: $3,795

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** |
| 312-50 CEH | Certified Ethical Hacker Training | 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

PROGRAM 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%

Certified Network Defender (CND)

PROGRAM 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.

program 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
* 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

Tuition and materials

Registration: $0  
Base Tuition: $3,316  
Materials: $379  
Total Tuition Fee: $3,695

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 |
| 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

program 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%

CompTIA Advanced Security Practitioner (CASP)

PROGRAM DESCRIPTION

This 5-day program is designed for people looking to start or enhance their careers as information security experts. You will build knowledge and skills in enterprise security, risk management and incident response, research and analysis, integration of computing, communications and business disciplines, as well as technical integration of enterprise components. Through this program, you will be expected to develop your knowledge of general security concepts, and the specific tools and procedures used to guard against intrusion, hacking, and cybercrimes. The program course material will center around these subject matter areas as they relate to the CASP certification objectives.

program OBJECTIVES

In this course, you will analyze and apply advanced security concepts, principles, and implementations that contribute to enterprise-level security. Students will learn:

* Manage risk in the enterprise.
* Integrate computing, communications, and business disciplines in the enterprise.
* Use research and analysis to secure the enterprise.
* Integrate advanced authentication and authorization techniques.
* Implement cryptographic techniques.
* Implement security controls for hosts.
* Implement security controls for storage.
* Analyze network security concepts, components, and architectures, and implement controls.
* Implement security controls for applications.
* Integrate hosts, storage, networks, and applications in a secure enterprise architecture.
* Conduct vulnerability assessments.
* Conduct incident and emergency responses.

Targeted Job Roles

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

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
* 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

Tuition and Labs

Registration: $0  
Base Tuition: $3,309  
Labs: $186  
Total Tuition Fee: $3,495

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** |
| CASP | CompTIA Advanced Security Practitioner | 40 |

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

REQUIRED TEXTBOOK

CompTIA Advanced Security Practitioner (CASP) CAS-003

Product Code: CASP0003-R10

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Cloud-based Lab exercises and labs

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM OUTLINE

**Day 1:**

**Chapter 1: Cybersecurity fundamentals**

Module A: Security concepts  
Module B: Risk management  
Module C: Threats and vulnerabilities

**Chapter 2: Recognizing vulnerabilities**

Module A: Common vulnerabilities  
Module B: Network vulnerabilities  
Module C: Application exploits

**Day 2:**

**Chapter 3: Vulnerability management**

Module A: Vulnerability assessment  
Module B: Vulnerability management programs

**Day 3:**

**Chapter 4: Reconnaissance**

Module A: Reconnaissance techniques  
Module B: Active reconnaissance  
Module C: Analyzing scan results

**Chapter 5: Monitoring networks**

Module A: Network security systems  
Module B: Logging and monitoring  
Module C: Network analysis

**Day 4:**

**Chapter 6: Policy design**

Module A: Security frameworks  
Module B: Security policies  
Module C: Controls and procedures

**Chapter 7: Secure network design**

Module A: Hardening networks  
Module B: Cryptography  
Module C: Hardening hosts and devices  
Module D: Secure application development

**Day 5:**

**Chapter 8: Identity management**

Module A: Identity systems  
Module B: Authentication technologies

**Chapter 9: Incident response**

Module A: Incident response planning  
Module B: Incident response procedures  
Module C: Forensic toolkits

GRADING

Grading will be assigned as follows:

* Student Attendance: 50%
* Student Participation in Lab Exercises: 50%

CAPM/PMP- IT Project Manager

PROGRAM 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 course 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 certifications 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 the first time. Each student will receive a student manual including review materials, key definitions and formulas, sample questions and answers.

Program 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
* In the event the applicant is unable to provide proof of secondary education, achieve a passing score on the Wonderlic Basic Skills Test.

PREREQUISITES

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

Tuition and Labs

Registration: $0  
Base Tuition: $3,156  
Labs: $139  
Total Tuition Fee: $3,295

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, an hour lunch break will be taken every day from 12:00PM to 1:00PM 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

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course 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 ten nights for evening students.

REQUIRED TEXTBOOK

Project Management Institute

PMBOK 6th Edition

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

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

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM 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 Certification
* 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: 50%
* Participation: 50%

ITIL v4 Foundations

##### Subject 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.

program 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
* 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

Tuition and Labs

Registration: $0  
Base Tuition: $2,243  
Labs: $52  
Total Tuition Fee: $2,295

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** |
| 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 |

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.

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM 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%

## Certified Information Systems Security Professional Training (CISSP)

PROGRAM DESCRIPTION

Welcome to *Certified Information Systems Security Professional (CISSP)®: Fourth Edition*. With your completion of the prerequisites and necessary years of experience, you are firmly grounded in the knowledge requirements of today’s security professional. This course will expand upon your knowledge by addressing the essential elements of the eight domains that comprise a Common Body of Knowledge (CBK)® for information systems security professionals. The course offers a job-related approach to the security process, while providing a framework to prepare for CISSP certification.

CISSP is the premier certification for today’s information systems security professional. It remains the premier certification because the sponsoring organization, the International Information Systems Security Certification Consortium, Inc. (ISC)2 ®, regularly updates the test by using subject matter experts (SMEs) to make sure the material and the questions are relevant in today’s security environment. By defining eight security domains that comprise a CBK, industry standards for the information systems security professional have been established. The skills and knowledge you gain in this course will help you master the eight CISSP domains and ensure your credibility and success within the information systems security field.

program OBJECTIVES

Students will learn:

* Analyze components of the Security and Risk Management domain.
* Analyze components of the Asset Security domain.
* Analyze components of the Security Engineering domain.
* Analyze components of the Communications and Network Security domain.
* Analyze components of the Identity and Access Management domain.
* Analyze components of the Security Assessment and Testing domain.
* Analyze components of the Security Operations domain.
* Analyze components of the Software Development Security domain.

Targeted Job Roles

* Security Auditors or Specialists
* Risk Management Professionals
* Network Admistrators
* Network Engineers

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
* 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

* Network +/Security + Certification or Equivalent Experience
* CyberSecurity Experience Highly Recommended
* Five Years Direct Work Experience Required for Certification

Tuition and Labs

Registration: $0  
Base Tuition: $3,423  
Labs: $72  
Total Tuition Fee: $3,495

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** |
| CISSP | Certified Information Security Systems Professional Training | 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 Information Systems Security Professional (CISSP): Fourth Edition

093024SC (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

PROGRAM OUTLINE

**Lesson 1: Security and Risk Management**

* Security Governance Principles
* Compliance
* Professional Ethics
* Security Documentation
* Risk Management
* Threat Modeling
* Business Continuity Plan Fundamentals
* Acquisition Strategy and Practice
* Personnel Security Policies
* Security Awareness and Training

**Lesson 2: Asset Security**

* Asset Classification
* Privacy Protection
* Asset Retention
* Data Security Controls
* Secure Data Handling

**Lesson 3: Security Engineering**

* Security in the Engineering Lifecycle
* System Component Security
* Security Models
* Controls and Countermeasures in Enterprise Security
* Information System Security Capabilities
* Design and Architecture Vulnerability Mitigation
* Vulnerability Mitigation in Embedded, Mobile, and Web-Based Systems
* Cryptography Concepts
* Cryptography Techniques
* Site and Facility Design for Physical Security
* Physical Security Implementation in Sites and Facilities

**Lesson 4: Communications and Network Security**

* Network Protocol Security
* Network Components Security
* Communication Channel Security
* Network Attack Mitigation

**Lesson 5: Identity and Access Management**

* Physical and Logical Access Control
* Identification, Authentication, and Authorization
* Identity as a Service
* Authorization Mechanisms
* Access Control Attack Mitigation

**Lesson 6: Security Assessment and Testing**

* System Security Control Testing
* Software Security Control Testing
* Security Process Data Collection
* Audits

**Lesson 7: Security Operations**

* Security Operations Concepts
* Physical Security
* Personnel Security
* Logging and Monitoring
* Preventative Measures
* Resource Provisioning and Protection
* Patch and Vulnerability Management
* Change Management
* Incident Response
* Investigations
* Disaster Recovery Planning
* Disaster Recovery Strategies
* Disaster Recovery Implementation

**Lesson 8: Software Development Security**

* Security Principles in the System Lifecycle
* Security Principles in the Software Development Lifecycle
* Database Security in Software Development
* Security Controls in the Development Environment
* Software Security Effectiveness Assessment

GRADING

Grading will be assigned as follows:

* Attendance: 50%
* Participation: 50%

## AWS re/Start Cloud Support CLASSROOM (AWS)

## AWS RE/START CLOUD SUPPORT HYBRID

Program Description

This skills development and training program prepares individuals for entry-level professional positions and careers in the cloud. Through real world, scenario-based learning, hands-on labs, and coursework, learners gain the technical skills they need for junior cloud roles. The program also focuses on building professional skills such as adaptive communication, time management, and collaboration. The program’s mission is to build a diverse pipeline of entry-level cloud talent.

Learning Objectives include:

* Working knowledge of operation systems like Linux, scripting, automation, programming languages and software lifecycles
* Understanding of networking concepts, protocols, security
* Knowledge of security fundamentals such as identity, authentication, authorization, AWS’ shared responsibility model and web access firewalls
* Fundamental understanding of databases concepts
* Application of core AWS services in the area of compute, storage and networking, including EC2, S3, IAM, VPC, Lambda, Cloud Formation, RDS, and Route 53
* Understanding of professional information technology working environment, including communication skills, collaboration tools, project management, presentation skills, project reporting, behavioral attitude

After program completion, each student will be prepared to sit for this highly coveted Amazon Web Services certification exam:

* AWS Certified Cloud Practitioner

Modality Versions

Our AWS re/Start Cloud Support Program is available in two modalities, AWS re/Start Cloud Support Hybrid and AWS re/Start Cloud Support Classroom.

For our Hybrid class version, students will be taught in real-time, with their questions addressed by a live instructor over audio, and in chat over a video meeting. 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.

For our classroom only version, students will be taught on campus with a live instructor with no option to attend virtually.

The content and instruction of both modalities is identical, the only difference is the delivery method.

Admission Requirements

Individuals applying for this program are required to:

* Be at least 17 years of age
* Interview with a Career Training Consultant
* Present proof of secondary education
* 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** |
| AWS-FCSO | AWS Fundamentals, Cloud & SysOps | 260/60/0/320 |

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

### Class Schedule

Day students will attend classes Monday through Friday from 9:00AM to 3:00 PM for 40 days. Students will have access to their Instructor in the classroom from 8am-9am, and 3:00pm-5:00pm each day for help with labs, exam prep, and project work. Classes for evening students will be held on Monday through Friday 7:00 to 11:00pm for 50 nights. 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 mealtime allowed but there will be two 10-minute breaks taken throughout the evening.

Tuition and Fees

Registration: $0  
Tuition: $13,875  
Materials: $0  
Total Tuition Fee: $13,875

Cost per Single Subject

|  |  |  |
| --- | --- | --- |
| **Subject Number** | **Subject Title** | **Cost** |
| AWS-FCSO | AWS Fundamentals, Cloud & SysOps | $13,875 |

Certification ExamS Required

* AWS Certified Cloud Practitioner

Targeted Job Roles

* IT Support – AWS Cloud
* IT Cloud Practitioner
* Jr. Network Administrator
* AWS Cloud Administrator
* Cloud DNS Specialist
* Cloud Security Specialist

Subject Descriptions and Syllabi

#### AWS Fundamentals, Cloud & Sys-OPS

SUBJECT DESCRIPTION

AWS re/Start focuses on two key technical areas IT Fundamentals and AWS Cloud. IT Fundamentals covers topics for support, operations, and automation roles such as Linux, networking, security, programming, Python and databases. AWS Cloud Fundamentals that highlights AWS core services, from introductory level to more in depth hands-on operational procedures. The technical portion of the curriculum is predominantly hands on and includes the end-to-end completion of a project from ideation to reporting, in order to exercise real life processes. In addition to technical skills, AWS re/Start teaches soft skills to prepare learners to succeed in a professional environment by preparing them to think critically, build multi-level projects, team dynamics, project planning, communication, and collaboration.

PERFORMANCE OBJECTIVES

Students will learn:

* Intro to IT
  + Linux Fundamentals
  + Networking Fundamentals
  + Security Fundamentals
  + Intro to Programming
  + Python Programming
  + Databases
* AWS Cloud Fundamentals
  + Cloud Concepts: What is Cloud Computing
  + Cloud Concepts: Cloud Economics
  + Cloud Concepts: AWS Global Infrastructure
  + AWS Core Services: Storage Services
  + AWS Core Services: Amazon Virtual Private Cloud (VPC)
  + AWS Core Services: Database Services
  + AWS Core Services: Load Balancing, CloudWatch, and Auto Scaling
  + AWS Cloud Security
  + Cloud Architecting
  + Cloud Support Services
* Systems Operations on AWS
  + Understanding Systems Operations on AWS
  + Tooling and Automation
  + Computing Servers
  + Computing Scaling and Name Resolution
  + Computing Containers and Serverless
  + Computing Database Services
  + Networking
  + Storage and Archiving
  + Monitoring and Security
  + Managing Resource Consumption
  + Creating Automated and Repeatable Deployments

Class Schedule

Day students will attend classes Monday through Friday from 9:00AM to 3:00 PM for 40 days. Students will have access to their Instructor in the classroom from 8am-9am, and 3:00pm-5:00pm each day for help with labs, exam prep, and project work. Classes for evening students will be held on Monday through Friday 7:00 to 11:00pm for 50 nights. 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.

REQUIRED COURSEWARE

* LeaderQuest Learning Management System Student Portal
* Amazon eBook
* Amazon Virtual Labs and Sandbox Lab Environment
* Amazon Practice Exams
* Embedded Assessments and Knowledge Checks

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Discussion
* Virtual labs
* Assessments
* Projects

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM OUTLINE

**Week 1**

**Day 1**

* Opening
* Welcome & Expectations
* Program Introduction
* Class Introductions and Curriculum Overview
* Vendor Introduction
* Self-Assessment
* Development Team and Roles
* Cloud Roles
* Career Goals
* Communication

**Day 2**

* Activity: Think Big
* Team Building/Settling
* Portfolio Project: Purpose and Brainstorming
* Introduction to AWS Training and Certification
* Team Building/Settling
* STAR Methodology
* Introduction to Linux
* Journaling (ACT)
* Open Discussion

**Day 3**

* Linux Recap
* Introduction to Linux Lab 1
* Team Building/Settling
* Linux Login Session
* Portfolio Project: Purpose & Brainstorming
* Discussion: Customer obsession
* Time Management
* Journaling (ACT)
* Open Discussion

**Day 4**

* Linux Login Session Lab 2
* Discussion: Ownership
* Portfolio Project: Purpose & Brainstorming
* Working with Files and Directories
* Lab 3: Working with Files and Directories
* Working with Text
* Journaling (ACT)
* Open Discussion

**Day 5**

* Lab 4: Working with Text
* Linux Users & Groups
* Lab 5: Linux Users & Groups
* Outlook
* Portfolio Project: Submission & Approval
* Managing File Permissions
* Lab 6: Managing File Permissions
* Journaling (ACT)
* Open Discussion

**Week 2**

**Day 1**

* Editing Files
* Lab 7: Editing Files
* Managing Processes
* Lab 8: Managing Processes
* Portfolio Project: Submission & Approval
* Managing Services
* Lab 9: Managing Services
* Discussion: Customer Obsession (cont’d)
* Managing Networking
* Journaling (ACT)
* Open Discussion

**Day 2**

* Lab 10: Managing Networking
* Software Management
* Lab 11: Software Management
* Linux Login Session
* Managing Log Files
* Working with Files
* The Bash Shell
* Lab 14: The Bash Shell

**Day 3**

* Linux Bash Shell Scripts
* Lab 15: Bash Shell Script
* Lab 1: Connect and Configure a Workstation
* Network Standards
* Ethernet Lan
* Lab 2: Wireshark
* Portfolio Project: PR/FAQ
* Journaling (ACT)
* Open Discussion

**Day 4**

* Ethernet Switching
* Lab 3: Examine Current Switch Configuration
* IP Addressing
* Lab 4: IP Addressing configuration
* IPV4 Subnetting
* Lab 5: Create a Subnetting Plan for a Small Network
* TCP and UDP
* Emotional Intelligence
* Management Protocol and Routing
* Lab 6: Examine ARP and DNS

**Day 5**

* Lab 7a: Examine DHCP
* Lab 7b: Examine Router Configuration
* Common Protocol
* Lab 8: Examine a Web Transaction – Wireshark
* Goal Setting
* Alumni Presentation with Students (in person or virtual)
* Portfolio Project: PR/FAQ
* Instructor’s Choice/Reinforced Learning
* Journaling (ACT)
* Open Discussion

**Week 3**

**Day 1**

* Digital Presence
* Discussion: Insist on the Highest Standards
* Network Security
* Lab 10: Research Anti-Malware
* Emerging Technologies
* Lab 11: Research MDM Software
* Presentation from Future Peers at Company
* Lab 0: Connecting to Vocareum Cloud Labs
* Introduction to Security

**Day 2**

* Lab 1: Increase your Security Awareness
* Working with Text
* Prevention: Network Discovery
* Lab 2: Interpret Scanning Results
* Prevention: Systems Hardening
* Lab 3: Harden Servers and Workstation
* Prevention: Security Architecture
* Lab 4: Security Architecture

**Day 3**

* Prevention: Network Hardening
* Lab 5: Explore Hardening Recommendations and Known Vulnerabilities
* Prevention: Data Security
* Lab 6: Protect Data
* Prevention: Public Key Infrastructure (PKI)
* Lab 7: Configure a PKI
* Portfolio Project: PR/FAQ
* Journaling (ACT)
* Open Discussion

**Day 4**

* Prevention: Identity Management
* Lab 8: Manage Passwords
* Detection
* Lab 9: Detect Malware
* Lab 10: Social Engineer
* Lab 11: Pen Testing
* Response
* Lab 12: Incident Response
* Analysis
* Lab 13: Monitor a System
* Lab 14: Review Legal Considerations
* Discussion: Think Big

**Day 5**

* Programming Basics
* Lab 1: Hello World
* Lab 2: Numeric Data Type
* Lab 3: String Data Type
* Lab 4: Lists, Tuple, Dictionary
* Portfolio Project: Requirements Gathering
* Instructor’s Choice
* Portfolio Project: PR/FAQ Submissions
* Journaling (ACT)
* Open Discussion

**Week 4**

**Day 1**

* Programming Basics
* Lab 5: Conditionals
* Lab 6: Loops
* Lab 7: Categorize Values
* Lab 8: Composite Data Types
* Lab 9: Create a Git Repository
* DevOps & Continuous Integration
* Configuration Management
* Lab 10: Explore the Value of Automation

**Day 2**

* Master Class
* Lab 11: Research Terraform
* Lab 12: Compare & Contrast Automation & Orchestration
* Debugging and Testing
* Lab 13: Evaluate a DevOps Tool
* Lab 14: Using the Debugger
* Meet Future Peers (in person or virtual)
* Python Fundamentals
* Lab 1: Prepare to Analyze Insulin with Python

**Day 3**

* Python Basics
* Activity 2-1; 2-2; 2-3
* Activity 2-4; 2-5; 2-6; 2-7; 2-8
* Discussion: Dive Deep
* Lab 2: Working with the String Sequence and Numeric Weight of Insulin
* Lab 14: Review Legal Considerations
* Portfolio Project: Requirements Gathering
* Journaling (ACT)
* Open Discussion

**Day 4**

* Functions
* Lab 3: Calculating the Net Charge of Insulin using Python
* Lab 4: Use Functions to Implement a Cesar Cipher
* Flow Control
* Activities in Flow Control
* Editing Files
* Modules and Libraries
* Activities: Modules and Libraries
* Lab 5: File Handler and Mod for Retrieving Information

**Day 5**

* Debugging and Testing
* Lab 6: Debugging Hello Worlds & Cesar Cypher
* Python and Sys Admin
* Lab 7: System Admin and Python
* Lab 7: System Admin and Python
* How to Apply and Discussion
* Challenge Lab: Bash Script and Review
* Instructor’s Choice
* Journaling (ACT)
* Open Discussion

**Week 5**

**Day 1**

* Database Fundamentals
* L1 – Database Fundamentals
* Lab 0: Installing the Pub 1 DB
* Lab 01: An Intro to DB
* Creating Tables and Learning Different Data Types
* Lab 2: Creating Tables and Learning Different Data Types
* Inserting Data into a Database
* Lab 3: Inserting Data
* Selecting Data from a Database
* Performing a Conditional Search
* Lab 05: Conditional Search

**Day 2**

* Working with Functions
* Lab 6: Working with Functions
* Organizing Data
* Lab 7: Organizing Data
* Retrieving Data
* Lab 8: Retrieving Data
* Indexes
* Lab 9: Indexes
* Updating/Deleting Tables
* Lab 10: Updating/Deleting Tables

**Day 3**

* Backup and Restore
* Lab 11: Backup and Restore
* Catch up on Databases
* Fact Finding: Databases
* Introduction: Cloud Foundations
* Teamwork & Collaboration
* Instructor’s Choice
* Journaling (ACT)
* Open Discussion

**Day 4**

* Introduction: Cloud Foundations
* Intro to Cloud Computing: Cloud Economics
* AWS Core Services – Compute
* Lab 01: Introduction to Amazon EC2
* Discussion: Have Backbone: Disagree and Commit
* Discussion: Invent and Simplify

**Day 5**

* Soft Skills: Networking
* Networking Event
* Instructor’s Choice
* Journaling (ACT)
* Open Discussion

**Week 6**

**Day 1**

* Networking Event
* AWS Core Services – Storage – 2
* Lab 2 Working with Amazon EBS
* AWS Core Services – Storage 3
* AWS Core Services – Storage 4
* P2P: Review Practicing Networking
* P2P: Review Practicing RACI
* AWS Core Services – Amazon VPC 1; Amazon VPC 2
* AWS Core Services – Amazon VPC 3

**Day 2**

* Lab 3: Build a VPC & Web Server
* AWS Core Services – Databases -0-1
* AWS Core Services – Databases -2
* Lab 4: Build your DB Server and Interact with Your DB Using an App
* Discussion: Bias for Action
* AWS Core Services – Load Balancing, Monitoring, Automatic Scaling -1 -2
* Lab 5: Scale & Load Balance Your Architecture
* Balancing, Monitoring, Automatic Master Class
* Group Discussion on Master Class

**Day 3**

* AWS Cloud Security – 1 through 8
* Cloud Architecting – 1 through 4
* Fact Finding: Cloud Foundations 1
* Fact Finding: Cloud Foundations Review
* Fact Finding: Well-Architected Framework
* Networking Event
* Journaling (ACT)
* Open Discussion

**Day 4**

* Networking Event
* AWS Billing Support – 1 through 3
* SysOps – Welcome and Overview
* Understanding SysOps -0 through -3
* Resume creation and Discussion
* Activity 1 – Install and Use the AWS CLI
* Tooling and Automation -1, -2
* Fact Finding – Billing and Review

**Day 5**

* Tooling and Automation -1, - 3
* Lab 1 – Using AWS Systems Manager
* How to Apply and Practice Discussion
* Activity 2 – Create a Website on Amazon S3
* Computing Servers – Computing AWS -1
* Lab 2 – Creating Amazon EC2 Instances
* Journaling (ACT)
* Open Discussion

**Week 7**

**Day 1**

* Challenge Lab: Linux EC2 Instance and Review
* Computing Servers – Computing on AWS -2
* Activity 3 – Troubleshoot Create Instance
* Computing (Scaling and Name Resolution) – 0 through – 3
* Lab 3 – Using AWS Auto Scaling
* Computing (Scaling and Name Resolution) – 4
* Activity 4 – Amazon Route 53 Failover Routing

**Day 2**

* Interview Settings and Practice
* Container – Serverless – 0 through 5
* Activity 5 – Working with AWS Lambda
* Discussion – Earn Trust
* Interview Process and Discussion
* Challenge Lab: Lambda Review
* Computing -db
* Activity 6 – Migrate to Amazon RDS
* Networking – 1 – 3
* Lab 4 – Configure a Amazon VPC

**Day 3**

* Activity 7 – Troubleshoot a Amazon VPC
* Storage and Archiving -1 through 6
* Elevator Pitch
* Activity 8 – Work with Amazon S3
* Challenge Lab: S3 and Review
* Interview Practice
* Open Discussion

**Day 4**

* Monitoring and Security – 1 through 3
* Lab 6 – Monitoring Infrastructure
* Activity 9 – Working with AWS CloudTrail
* Discussion – Deliver Results
* Managing Resource Consumption – 0 through 3
* Lab 7 – Managing Resources
* Activity 10 – Optimize Utilization
* Prep for Practice Test
* Configuration Management – 0 through 6
* Networking Event

**Day 5**

* Lab 8 – Automation with AWS CloudFormation
* Fact Finding – CloudFormation
* Challenge Lab: CloudFormation
* Challenge Lab: Database
* Review Fact Finding and Labs
* Prep for Practice Test
* Troubleshooting AWS CloudFormation
* Continuous Improvement Continuous Integration
* Activity 8: Project Scenario
* Practice Test
* Open Discussion

**Week 8**

**Day 1**

* Prep for Practice Test
* Company Visit

**Day 2**

* Cloud Practitioner Essential Digital, Interview Skills, Resume Review
* Presentation Skills, Presence, Project Presentation
* Review Product FAQ, Review AWS Whitepapers,
* Review Exam Blueprint, Mock Exam and Review

**Day 3**

* Cloud Practitioner Essential Digital, Interview Skills, Resume Review
* Presentation Skills, Presence, Project Presentation
* Review Product FAQ, Review AWS Whitepapers,
* Review Exam Blueprint, Mock Exam and Review
* Open Discussion

**Day 4**

* Cloud Practitioner Essential Digital, Interview Skills, Resume Review
* Presentation Skills, Presence, Project Presentation
* Review Product FAQ, Review AWS Whitepapers,
* Review Exam Blueprint, Mock Exam and Review

**Day 5**

* Practice Exam Day

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, Director of Compliance

Signature: Meghan Jurado, 1/26/2021

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)