

ACI Learning

8663 Baypine Road. Bldg. 4 Suite 104.

Jacksonville, FL 32256

Phone: (904) 399-3555

Catalog Number 4, Volume Number 5, Revised 8/19/2021

ACI Learning is licensed by the Commission for Independent Education, Florida Department of Education. Additional information regarding this institution may be obtained by contacting the Commission at 325 West Gaines St., Ste. 1414, Tallahassee, FL 32399-0400, toll-free (888) 224-6684

Certified true, correct in Content and Policy

Meghan Jurado, Director of Compliance

Contents

[Introduction 3](#_Toc80001278)

[Administration Staff 4](#_Toc80001279)

[Faculty 5](#_Toc80001280)

[Programs Offered 7](#_Toc80001281)

[Tuition 10](#_Toc80001282)

[Class Schedule 11](#_Toc80001283)

[Full time Students: 11](#_Toc80001284)

[Part-Time Students: 11](#_Toc80001285)

[Asmission Requirements 11](#_Toc80001286)

[Enrollment 12](#_Toc80001287)

[ACI Live Online offerings 12](#_Toc80001288)

[Facilities 12](#_Toc80001289)

[Career services 13](#_Toc80001290)

[Attendance Requirements 13](#_Toc80001291)

[ACI Learning Make-Up Work Policy 13](#_Toc80001292)

[Leave of Absence Policy 13](#_Toc80001293)

[VA Benefit Disbursement DELAYS 14](#_Toc80001294)

[Certification Policy 14](#_Toc80001295)

[Grading System/Progress Reports 15](#_Toc80001296)

[Re-Admission Policy 15](#_Toc80001297)

[Graduation Policy 15](#_Toc80001298)

[Reschedule Policy 16](#_Toc80001299)

[Cancellation and Refund Policy 16](#_Toc80001300)

[Conduct Policy 18](#_Toc80001301)

[Student Complaints 18](#_Toc80001302)

[Student Services 19](#_Toc80001303)

[Previous Credits 19](#_Toc80001304)

[Record keeping 19](#_Toc80001305)

[Dismissal 19](#_Toc80001306)

[Student Grievance Procedure 19](#_Toc80001307)

[Programs 20](#_Toc80001308)

[Computer User Support SPECIALIST 20](#_Toc80001309)

[COMPUTER USER SUPPORT SPECIALIST HYBRID 20](#_Toc80001310)

[Cybersecurity Specialist 42](#_Toc80001311)

[Network Support Specialist 52](#_Toc80001312)

[CCNA 1 & 2: Certified Cisco Network Administrator, CCNA Prep 60](#_Toc80001313)

[CISCO Certified Network Associate PREP 61](#_Toc80001314)

[Technical support specialist 64](#_Toc80001315)

[Information Security Analyst 78](#_Toc80001316)

[CompTIA NETWORK+ prep 88](#_Toc80001317)

[CompTIA Security+ prep 92](#_Toc80001318)

[EC-COUNCIL CERTIFIED ETHICAL HACKER prep - (CEH) 97](#_Toc80001319)

[CERTIFIED NETWORK DEFENDER prep- (CND) 101](#_Toc80001320)

[COMPUTER HACKING FORENSIC INVESTIGATOR prep - (CHFI) 104](#_Toc80001321)

[EC-COUNCIL CERTIFIED ENCRYPTION SPECIALIST prep-(ECES) 108](#_Toc80001322)

[COMPTIA ADVANCED SECURITY PRACTITIONER prep- (CASP) 111](#_Toc80001323)

[Itil foundations Certification prep 114](#_Toc80001324)

[Comptia a+ certification prep 119](#_Toc80001325)

[Senior technology Project MANAGER - (STPM) 130](#_Toc80001326)

[CAPM & PMP IT project manager Prep 138](#_Toc80001327)

[Certified Information Systems Security Professional prep- (CISSP) 142](#_Toc80001328)

# Introduction

LeaderQuest Holding purchased ConsulTech in October 2015. In 2019, Misti and LeaderQuest joined teams and renamed the school Audit, Cyber, Information Technology Learning (ACI Learning). 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 credential standard in their field of specialty.

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

The School is headquartered in Centennial, CO and as of this writing, offers class on five campuses: Englewood, CO; Colorado Springs, Co; Jacksonville, FL; Irving TX and San Antonio TX.

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 Centennial, Colorado.
* July 2006: School is sold to new ownership. The acquiring company is LeaderQuest with one majority shareholder in George Cohlmia. School continues to operate as Hensmann Training and Education Centers through 2006 and into early 2007.
* April 2007: School officially changes its name from Hensmann Training and Education Centers to LeaderQuest.
* October 2014: Irving Dallas school is opened and approved by the Texas Workforce Commission
* October 2015: Purchased ConsulTech Inc. in Jacksonville, FL and is approved by Florida Department of Education.
* November 2016: Consultech’s name changed to LeaderQuest IT Training
* July 2018: LeaderQuest San Antonio is approved by the TWC.
* July 2019: MISTI takes control of LeaderQuest, all staff and programs are retained.
* Sept 2020 Leaderquest IT Training’s name changed to ACI Learning. (ACI Learning is a fictitious name registered to LeaderQuest Holdings)

# Administration Staff

Key Administrative Staff:

* Brett Shively - CEO & Owner
* Jennifer Mathis– Campus Director – Jacksonville
* Maria Smith – Senior Compliance Specialist/Lead SCO
* Meghan Jurado- Director of Compliance

Jacksonville Staff:

* Brittany Molineux- Frontline Associate (Days)
* Zsakituh Goodmond- Frontline Associate (Nights)
* John Beverly – Career Training Consultant
* Michelle Biernat- Career Training Consultant
* Jeff Reid – Career Training Consultant
* Tiffany Murphy- Career Training Consultant
* Bridget Scrogham- Employment Development Manager
* Brian Morgan-Employment Development Manager

# Faculty

**John Brown – Adjunct Instructor**

John has a strong background managing technical staff as well as personal skills in technical support. John has 30+ years of info tech experience, in every aspect of IT, including operator, programming, database management, desktop support, server support, network design and support. John possesses a Bachelor of Science, Computer & Information Sciences, (College of Engineering, University of Florida), Professional Engineer, and Industrial ITILCertification.

John currently instructs the following programs:

* + - **Computer User Support Specialist**
    - **ITIL V3 Foundations Prep**
    - **CompTIA A+ Prep**
    - **CompTIA Network + Prep**
    - **CompTIA Security + Prep**
    - **Technical Support Specialist**

**Robert Fleming- Adjunct Instructor**

IT professional with 11 years of experience working in various roles from support, education, onsite assistance, and help desk. He has a Bachelor of Science from University of South Florida major in Information Systems Management. Robert has 3 years in professional marketing focusing on field team management, analyzing current consumer trends, and ensuring success of product launch campaigns. Proven at building internal and external customer value, communicating professionally and effectively. Robert currently instructs the following programs

* **Network Support Specialist**
* **Cisco Certified Network Associate (CCNA)**

**Jay Walker–Technical Instructor**

Jay possesses a wide array of technology certifications. Jay has a Bachelor of Science in Information Technology from Western Governors University. Jay currently instructs the following programs

* + - **Computer User Support Specialist**
    - **CompTIA A+ Prep**
    - **Technical Support Specialist**

**Roderick Fedd – Technical Instructor**

Rodderick worked in the IT field for over 5 years. Rodderick possesses a wide array of technology certifications. Roderick has a Bachelor of Science in Information Technology from Phoenix University and Information Technology from Omni Tech Institute. Roderick currently instructs the following programs

* + - **Computer User Support Specialist**
    - **CompTIA A+ Prep**
    - **CompTIA Network + Prep**
    - **CompTIA Security + Prep**
    - **Technical Support Specialist**

**Marcia Ingino – Adjunct Instructor**

Marcia has been teaching project management and business analysis for over 16 years where she’s maintained an aggregate evaluation score of 9.2 of 10.0. Marcia possesses a BS in Computer Engineering from University of Illinois and an MS in Engineering Management from University of Colorado. Marcia currently instructs the following programs:

* **STPM – Senior Technology Project manager**
* **CAPM & PMP IT Project Manager Prep**

**Randy Kohler- Adjunct Instructor**

Randy has many years of extensive hands-on experience in network, telecommunication and systems administration. Randy currently instructs the following programs

* **CompTIA Security+ Prep**
* **CompTIA Network + Prep**

**Larry Coldiron- Adjunct Instructor**

Larry has 23 years in the US Navy with an extensive desktop support experience; He has experience working hands-on with real world experience in several areas of IT. Larry currently instructs the following programs

* **Computer User Support Specialist**
* **ITIL V3 Foundations Prep**
* **CompTIA A+ Prep**
* **CompTIA Network + Prep**
* **Technical Support Specialist**
* **Network Support Specialist**
* **Cisco Certified Network Associate (CCNA)**

**Edward Spencer- Adjunct Instructor**

Highly qualified and adaptive network and security analyst with more than 10 years’ experience on a wide variety of technologies with a focus on security, compliance, diversity, interoperability, risk management, process improvement, strategic vision, and support of the business. Edward currently instructs

* **Computer User Support Specialist**
* **CompTIA A+ Prep**
* **CompTIA Network+ Prep**
* **CompTIA Security + Prep**
* **Technical Support Specialist**

**Robert Brad Leppla - Adjunct Instructor**

Robert possesses a wide array of technology certifications. Robert has a master in Computer Information Resources from Webster University, and a Master’s degree in Computer Science from Colorado Technical University.

* **Cisco Certified Network Associate (CCNA)**
* **Network Support Specialist (NSS)**

**John Guise- Adjunct Instructor**

John has over 21 years in the education industry. He possesses a Master of Science in Information Security and Assurance Western Governors University a BS in Computer Information Systems as well a AAS Information Technology. John instructs

* + - **Computer User Support Specialist**
    - **CompTIA Network+ Prep**
    - **CompTIA Security + Prep**
    - **Computer Hacking Forensic Investigator**

# Programs Offered

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Program Title / Certificate | Course Number | Course Title | Contact Hours (Hrs) | Program Completion Length\* (Days) |
| **Infrastructure and Tech Support** | | | | |
| Computer User Support Specialist (CUSS) | ITIL | ITIL Foundation Certification Prep | 40 | 45 |
| 220-1001 | CompTIA A+ Essentials Core 1 Prep | 40 |
| 220-1002 | CompTIA A+ Practical Applications Core 2 Prep | 40 |
| N10-007 | CompTIA Network+ Prep | 40 |
| SY0-601 | CompTIA Security+ Prep | 40 |
| Cisco Certified Network Associate  (CCNA) | CCNA 1 | Certified Cisco Network Administrator, CCNA Part 1 Prep | 40 | 10 |
| CCNA 2 | Certified Cisco Network Administrator, CCNA Part 2 Prep | 40 |
| Network Support Specialist (NSS) | N10-007 | CompTIA Network+ Prep | 40 | 30 |
| SY0-601 | CompTIA Security+ Prep | 40 |
| CCNA 1 | Certified Cisco Network Administrator, CCNA Part 1 Prep | 40 |
| CCNA 2 | Certified Cisco Network Administrator, CCNA Part 2 Prep | 40 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | Technical Support Specialist (TSS) | ITIL | ITIL Foundation Certification Prep | 40 | 25 | | 220-1001 | CompTIA A+ Essentials Core 1 Prep | 40 | | 220-1002 | CompTIA A+ Practical Applications Core 2 Prep | 40 | | ITIL Foundations Prep | ITIL | ITIL Foundation Certification Prep | 40 | 5 | | CompTIA A+ Certification Prep | 220-1001 | CompTIA A+ Essentials Core 1 Prep | 40 | 10 | | 220-1002 | CompTIA A+ Practical Applications Core 2 Prep | 40 | | CompTIA Network + Prep | N10-007 | CompTIA Network + Prep | 40 | 5 | | CompTIA Security + Prep | SY0-601 | CompTIA Security + Prep | 40 | 5 | | | | | |
| **Information Security** | | | | |
| Cybersecurity Specialist (CYBER) | SY0-601 | CompTIA Security + Prep | 40 | 25 |
| 312-50 | EC-Council Certified Ethical Hacker Prep | 40 |
| 312-49 | Computer Hacking Forensics Investigator | 40 |
| Information Security Analyst (ISA) | SY0-601 | CompTIA Security+ Prep | 40 | 30 |
| 312-38 | Certified Network Defender Prep | 40 |
| 312-50 | EC-Council Certified Ethical Hacker Prep | 40 |
| EC-Council Certified Ethical Hacker Prep (CEH) | 312-50 | EC-Council Certified Ethical Hacker Prep | 40 | 5 |
| Certified Network Defender Prep (CND) | 312-38 | Certified Network Defender Prep | 40 | 5 |
| Computer Hacking Forensic Investigator Prep (CHFI) | 312-49 | Computer Hacking Forensic Investigator Prep | 40 | 5 |
| EC-Council Certified Encryption Specialist Prep (ECES) | 212-81 | EC-Council Encryption Specialist Prep | 24 | 3 |
| CompTIA Advanced Security Practitioner Prep (CASP) | CASP-002 | CompTIA Advanced Security Practitioner Prep | 40 | 5 |
| Certified Information Systems Security Professional Prep (CISSP) | CISSP | Certified Information Systems Security Professional Prep | 40 | 5 |
| **Project and Service Management** | | | | |
| Senior Technology Project Manager (STPM) | ITIL | ITIL Foundation Certification Prep | 40 | 10 |
| CAPM/PMP | CAPM & PMP IT Project Manager Prep | 40 |
| CAPM & PMP IT Project Manager Prep | CAPM/PMP | CAPM & PMP IT Project Manager Prep | 40 | 5 |

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

# Tuition

|  |  |
| --- | --- |
| **Programs** | **Tuition:** |
| Technical Support Specialist (TSS) – 120 hours | $8,085 |
|  | |
| Computer User Support Specialist (CUSS) – 200 hours | $13,875 |
|  | |
| Cisco Certified Network Associate (CCNA) – 80 hours | $6,590 |
|  | |
| Network Support Specialist (NSS) – 160 hours | $12,830 |
|  | |
| Information Security Analyst- (ISA)- 120 hours | $10,485 |
|  | |
| Cybersecurity Specialist (CYBER) – 120 hours | $10,485 |
|  | |
| CompTIA Security + Prep (Sec +) – 40 hours | $2,895 |
|  | |
| Installing & Configuring Windows Server 2012 (SA) – 120 hours | $8,895 |
|  | |
| EC Council Certified Encryption Specialist (ECES) -24 hours | $2,545 |
|  | |
| Computer Hacking Forensic Investigator Prep (CHFI) – 40 hours | $3,795 |
|  | |
| CompTIA Advanced Security Practitioner Prep (CASP)- 40 hours | $3,495 |
|  | |
| Certified Ethical Hacker Prep (CEH) – 40 hours | $3,795 |
|  | |
| Certified Network Defender Prep(CND) – 40 hours | $3,795 |
|  | |
| CompTIA Network+ Prep (Net+) – 40 hours | $2,895 |
|  | |
| CompTIA A+ Certification Prep (A+)- 40 hours | $5,790 |
|  | |
| ITIL Foundations Prep (ITIL) -40 hours | $2,295 |
|  | |
| Senior Technology Project Manager (STPM) – 80 hours | $5,590 |
|  | |
| CAPM & PMP IT Project Manager Prep(PMP)-40 hours | $3295 |
|  | |
| Certified Information Systems Security Professional Prep (CISSP)- 40 hours | $3,495 |

# Class Schedule

ACI Learning is very flexible in scheduling students. ACI Learning has ongoing enrollments, which start every two months.

All courses are determined by Vendor standards.

## Full time Students:

Monday through Friday 8:00am – 5:00pm with one-hour lunch break, 8:00 am - 12:00 pm for mornings or 1:00pm - 5:00 pm for afternoons. Full time is 20 hours per week.

Some Saturdays are allowed for make-up, from 7:30 am to 4:30 pm.

## Part-Time Students:

Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break.

Some Saturdays are allowed for make-up, from 7:30 am to 4:30 pm.

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:

Week of New Year’s Labor Day

Memorial Day Week of Thanksgiving

Independence Day Week of Christmas

# Asmission Requirements

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

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

# Enrollments

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.

Students will be notified of any changes made at the institution within a reasonable timeframe.

# ACI Live Online offerings

ACI Learning offers the opportunity to attend our classes in a live, 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.

Prospective students may enroll anytime. Student are able to switch to onsite classes at any time. An overall attendance of at least 80% is required to be considered passing. 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 present or absent and the amount of hours attended. If attendance falls under 80% the student will be considered failing and have to set up a retake of their course through student services.

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

Certification attempts are available through 3rd party testing companies remotely or students can be scheduled onsite at our facility or a facility closest to the student.

# Facilities

The Jacksonville campus located at 8663 Baypine Road Bldg. 4 Ste. 104 Jacksonville, FL 32256 in 5,959 sq. feet with an inviting campus atmosphere where modern conveniences blend into the surroundings, including walking paths, a spring-fed lake with overlooking decks. Hours of operation are from 8am - 12am. All classrooms are set up with the latest state-of-the-art equipment and furniture. Pearson VUE testing center is also located onsite. There is also a designated break area where coffee and drinks are furnished.

The ACI Learning main corporate office is located in Denver at 6855 S Havana St #280, Englewood CO 80112. ACI Learning also operates a facility in Colorado Springs at 7222 Commerce Center Dr. Colorado Springs 80919 as well as Irving, TX 102 Decker Ct, Irving TX 75062 and San Antonio TX at 8200 I-H 10 West Suite 801, 78230. Hours of operation are from 8 am to 5 pm. ACI is a smoke-free environment. For those that smoke, designated smoking areas are located outside our training facilities.

# Career services

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 of at least 80% is required to be considered passing. Students are required to use a Biometric fingerprint reader to record attendance. In addition to biometric fingerprint reader, 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 present or absent. If attendance falls under 80% the student will be considered failing and have to set up a retake of their course through student services.

Any student that falls below 80% attendance while in a Program will be terminated from that program and the last date of attendance will be recorded. If a student wishes to re-enroll into the Program, the student will be re-enrolled and give prior credit for any of the classes that were previously attended.

If students using VA benefits exceeds 20% total absences per period, they will be required to take the course until they meet the required amount of hours for certification. Students will have a limited number of reschedules to pass available to them, evaluated on a case-by-case basis.

# ACI Learning Make-Up Work Policy

At ACI Learning, we understand that there are circumstances beyond a participant’s control that may lead to missed class time. To achieve the 100% attendance required to best absorb course materials and labs, we offer a limited make-up policy to accommodate students with mitigating circumstances (e.g. medical emergencies.).

To request a make-up session, please send an email to Client Services at [client.services@acilearning.com](mailto:client.services@acilearning.com) outlining your request within 24 hours of missed class time. Requests are subject to approval and may be denied, and each request must be documented in the student file. Once your make-up session has been approved by the campus and Compliance, your session will be set up with our Instructor Mentor, who will ensure that all material is covered and any assignments that were missed can be reviewed. Once the session is completed it will be noted in the student file and the attendance will be updated when appropriate. Any work missed must be made up within five business days.

# Leave of Absence Policy

Students who are unable to continue classes for medical reasons or approve extenuating circumstances (medical or otherwise) will be required to take a leave of absence until that are able to return to class. A student should contact clientservices@acilearning.com to request a leave of absence, stating the reasons in writing with any applicable documentation, and the request will be reviewed and grated in writing. Proper documentation will be required to substantiate a student’s withdrawal. Students can come and refresh any class on a space availability basis for the life of the course.

# VA Benefit Disbursement DELAYS

Any covered individual wishing to attend classes using their Chapter 33 or Chapter 31 benefits 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 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 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 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. These attempts are not charged in tuition or fees. Students are eligible to schedule a certification attempt appointment after completing each class in their program. The following policy statements outline conditions and requirements associated with certification:

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

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

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 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’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 70% 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 requirement or will be terminated at that time.

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.

Course Numbers are based on the current version of the approved course.

A clock hour is a period of 60 minutes with at least 50 minutes of instruction or lab time under supervision of an instructor.

# 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 and may reenroll on the next program start date. Such reenrollment does not circumvent the approved refund policy.

# Graduation Policy

Upon successful completion of program, students will receive a Diploma. 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 ’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 Students will be dropped from their program and provided a refund for the remaining classes per the cancellation policy below.

# Cancellation and Refund Policy

Cancellation can be made in person, by electronic mail, or by telephone. A full refund will be made to any student who cancels the enrollment contract within 3 Business Days, excluding Saturdays, Sundays and legal holidays) whichever is sooner after the enrollment contract is signed, except that the school may retain not more than $150 in any administrative fees charged, as well as items of extra expense that are necessary for the portion of the program attended and stated separately on the enrollment agreement.

**Refund Policy**

1. Refund computations will be based on scheduled course time of class attendance through the last date of attendance. A full refund will be made to any student who cancels enrollments within three business days without penalty. Refund will be based on the remaining portion of class that was not attended.  Students will not be charged for classes that was not taken. Written/Approved Leaves of absence, suspensions and school holidays will not be counted as part of the scheduled class attendance. More simply, the refund is based on the precise number of course time hours the student has paid for, but not used, at the point of termination, up to the 75% completion mark, after which no refund is due.

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

(a) The last day of recorded attendance or date of official notice, if the student is terminated by the school;

(b) The date of receipt of notice from the student

3. If tuition is collected in advance of entrance, and if after expiration of the 72-hour cancellation privilege the student does not enter school, not more than $150 in any administrative fees charged shall be retained by the school for the entire program.

4. Refunds for items of extra expense to the student, such as books, tools, or other supplies are to 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.

5. 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.

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

(a) An enrollee is not accepted by the school;

(b) If the course of instruction is discontinued by the school and this prevents the student from completing the course; or

(c) 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.*

#### **VETERANS REFUND POLICY**

1. Veterans not accepted by the school and who cancel this contract by notifying the school within 3 business days is entitled to a full refund of all tuition paid. Veterans, who withdraw after three business days, but before commencement of classes, are entitled to a full refund of all tuition and fees paid. In the case of veterans withdrawing after commencement of classes, the school will retain a percentage of tuition, which is based on the ratio of total number of hours in the course. The refund is based on the last date of recorded attendance.

**REFUND POLICY FOR STUDENTS CALLED TO ACTIVE MILITARY SERVICE**

2. 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 Florida 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.

3. The payment of refunds will be totally completed such that the refund instrument has been negotiated or credited into the proper account(s), within 30 days after the effective date of termination.

***ALL STUDENTS***

* 1. The student may cancel this contract at any time prior to midnight of the third business day after signing this contract, without penalty.
  2. The effective date of termination for refund purposes will be the earliest of the following:

(a) The last day of recorded attendance or date of official notice, if the student is terminated by the school;

(b) The date of receipt of notice from the student

* 1. The student will receive a full refund of tuition and fees paid if the school discontinues a course program within a period of time a student could have reasonably completed it, except that this provision shall not apply in the event the school ceases operation.
  2. The payment of refunds will be totally completed such that the refund instrument has been negotiated or credited into the proper account(s), within 30 days after the effective date of termination.
  3. Complaints, which cannot be resolved by direct negotiation between the student and the school, may be filed online with the Florida Department of Education. There is a two-year limitation (from the students last date of attendance) on the Division taking action on student complaints. DOE can be reached at (888) 224-6684 or a complaint can be filed online at <http://www.fldoe.org/policy/cie/file-a-complaint.stml>.
  4. The policy for granting credit shall not impact the refund policy.

# 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. In Jacksonville, the Florida Department of Education can be reached at (888) 224-6684 or a complaint can be filed online at <http://www.fldoe.org/policy/cie/file-a-complaint.stml>. All student complaints must be submitted to the school and Division in writing:

Commission for Independent Education 325 W. Gaines Street, Suite 1414  
Tallahassee, FL. 32399-0400

There is a two-year limitation on Division action on student complaints.

Note: Documents received in this office are considered public record. Confidentiality cannot be guaranteed. This office cannot give legal advice to any individual or take any legal action on behalf of any individual. We will investigate your complaint to see what assistance, if any, we may be able to offer.

# Student Services

ACI Learning’s primary educational format is traditional classroom instruction.

Each ACI Learning training facility offers students a break room and a study area for their convenience. Instructors are available for test preparation review & counseling on skills development necessary in the technical job market. Employment assistance is given by the school faculty to students. ACI will notify any students of job availability and refer them to area business contacts. Instructors are available as a technical reference. ACI cannot guarantee employment. Progress is readily available to students via their test results.

# 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.

The school maintains a written record of the previous education and training of the veteran or eligible person and clearly indicates that appropriate credit has been given for previous education and training, with the training period shortened proportionately, and the veteran or eligible person and the Department of Veterans Affairs so notified.

# Record keeping

VA students’ records must be kept for 3 years following the ending date of the last period certified to VA. Records need to be kept longer than 3 years only if a written request to keep the records longer is received from the Department of Veterans Affairs or the General Accounting Office 30 or more days before the end of the 3-year period. This requirement is in the Code of Federal Regulations (38 CFR 21.4209(f)).

# Dismissal

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

# Student Grievance Procedure

Students can bring any grievance to the attention of the school in order for the school to help resolve any issues that may occur. Grievances should be sent via email to the School Training Director at jenn.mathis@acilearning.com

Any grievances unresolved by the school should be sent to:

Commission for Independent Education 325 W. Gaines Street, Suite 1414  
Tallahassee, FL. 32399-0400

Or E-mail: [cieinfo@fldoe.org](mailto:cieinfo@fldoe.org)   
Or Fax: 850-245-3238

All student records are kept secure in a locked room and are only assessable to ACI employees. All student can request a copy of his or her records by submitting an email to clientservices@acilearning.com

# Programs

Computer User Support SPECIALIST

## COMPUTER USER SUPPORT SPECIALIST HYBRID

### Program Description

This program will provide students with the skills and knowledge necessary to install, build, maintain, and configure personal computers, laptop computers, and printers. They will also learn the principles of physical and TCP/IP networks. Finally, they will learn operational and professional procedures as an IT technician.

Students will also learn how to support personal computers, mobile devices, and small networks in a business setting, including hardware and software troubleshooting, Windows installation and configuration, networking, and security.

Additionally, students will receive foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network. Students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field.

Finally, based on the ITIL best practice service lifecycle approach, this program provides practical understanding of the key concepts, principles, processes, and functions that enables successful IT Service Management (ITSM) provision. 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 Examination.

The Computer User Support Specialist program is available online via Zoom Platform for lectures in which students interact live with faculty. Assessments and Resources (labs, test preps) will be conducted through our Learning Management System online modality.

### Course Objective

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:

* 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.
* The program also introduces the principles and core elements of IT service management (ITSM) based on ITIL framework

The Computer User Support Specialist program is available online via Zoom Platform for lectures in which students interact live with faculty. Assessments and Resources (labs, test preps) willalso be conducted through our Learning Management System online modality. Faculty on a daily basis will take attendance

### 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

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| ITIL | ITIL Foundation Certification Prep | 20/20/0/40 |
| 220-1001 | CompTIA A+ Essentials Core 1 Prep | 20/20/0/40 |
| 220-1002 | CompTIA A+ Practical Applications Core 2 Prep | 20/20/0/40 |
| N10-007 | CompTIA Network+ Prep | 20/20/0/40 |
| SY0-601 | CompTIA Security+ Prep | 20/20/0/40 |

The approximate time required to complete this program is 45 days for day students and 50 days for evening students.

### Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00 PM for 5 days, and from 8:00 am to 12:00 pm or 1:00pm to 5:00 pm for 40 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For full day students, an hour lunch break will be taken every day from 12:00PM to 1:00PM with four 10 minutes breaks dispersed throughout the day. For morning/afternoon/evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

### Tuition

$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

#### Subject 220-1001: CompTIA A+ Essentials Prep

#### Subject Description

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

##### Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab
* 0 hours externship

##### Course Objectives

* Upon 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.

Who Should Attend

The target student is anyone with basic computer user skills who is interested in obtaining a job as an IT professional or PC technician. Possible job environments include mobile or corporate settings with a high level of face-to face client interaction, remote-based work environments where client interaction, client training, operating systems, and connectivity issues are emphasized, or settings with limited customer interaction where hardware activities are emphasized. In addition, this course will help prepare students to achieve a CompTIA A+ Certification.

##### Prerequisites

Candidates should have the knowledge required to understand the fundamentals of computer technology, networking, and security. They should be able to identify hardware, peripheral, networking, and security components. They should also understand the basic functionality of the operating system and basic troubleshooting methodology.

##### Requird Textbooks

CompTIA A+ Essentials Core 1 (220-1001)

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 3/3/2020

##### Instructional Methods

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

##### Maximum Student to Instructor Ratio

20:1

##### 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 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.

#### Subject 220-1002: A+ Practical APPLICATIONS PREP

##### Subject 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+ Practical Applications 220-1002 Certification Exam

##### Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab

##### Course Objectives

After completing this course, students will be able to:

* 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

##### Prerequisites

Candidates should have the knowledge required to understand the fundamentals of computer technology, networking, and security. They should be able to identify hardware, peripheral, networking, and security components. They should also understand the basic functionality of the operating system and basic troubleshooting methodology.

##### Required Textbooks

CompTIA A+ Practical Applications Core 2 (220-1002)

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 3/3/2020

##### Instructional Methods

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

##### Maximum Student to Instructor Ratio

20:1

#### 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 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.

Subject N10-007: Network+

##### Subject Description

This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network.

##### 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 basic components of network theory.
* Identify the major network communications methods.
* Identify network data delivery methods.
* List and describe network media and hardware components.
* Identify the major types of network implementations.
* Identify the components of a TCP/IP network implementation.
* List the major services deployed on TCP/IP networks.
* Identify characteristics of a variety of network protocols.
* Identify the components of a LAN implementation.
* Identify the components of a WAN implementation.
* Identify major issues and technologies in network security.
* Identify the components of a remote network implementation.
* Identify major issues and technologies in disaster recovery.
* Identify major data storage technologies and implementations.
* Identify the primary network operating systems.
* Identify major issues, models, tools, and techniques in network troubleshooting.

##### Prerequisites

A typical student taking up the CompTIA® Network+® (N10-007) course should have a minimum of nine months or more of professional computer support experience as a PC or help desk technician. Networking experience is helpful but not mandatory; A+ certification or equivalent skills and knowledge is helpful but not mandatory.

##### Textbooks / Courseware

CompTIA Network+ N10-007

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 3/3/2020

##### Instructional Methods

* Lecture
* Overhead slides
* Lab

##### Maximum Student to Instructor Ratio

20:1

##### 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%
* Lab Assignments: 50%

#### Subject SY0-601: COMPTIA Security+Prep

##### 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.

#### Subject ITIL-FND: ITIL Foundation certification Prep

##### 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 Date 2019

##### 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%

Cybersecurity Specialist

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.

After program completion, student will have sat through three highly coveted information security certifications:

* CompTIA Security+
* EC-Council Certified Ethical Hacker (CEH)
* Computer Hacking Forensic Investigator (CHFI)

Learn the details behind the investigation of computer logs, network traffic, wireless attacks, and web attacks.

Admission Requirements

Individuals applying for this program are required to:

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

Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| SY0-601 | CompTIA Security+ Prep | 20/20/0/40 |
| 312-50 | EC-Council Certified Ethical Hacker Prep | 20/20/0/40 |
| 312-49 | Computer Hacking Forensics Investigator Prep | 20/20/0/40 |

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

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00 PM for 5 days, and from 8:00 am to 12:00 pm or 1:00pm to 5:00 pm for 20 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For full day students, an hour lunch break will be taken every day from 12:00PM to 1:00PM with four 10 minutes breaks dispersed throughout the day. For morning/afternoon/evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

Tuition

$10,485

Targeted Job Roles

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

Subject Descriptions and Syllabis

#### Subject SY0-601: COMPTIA Security+Prep

##### 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.

Subject 312-50: ec-council Certified Ethical Hacker prep

Subject 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 leaves this intensive 5-day class, you will have hands on understanding and experience in Ethical Hacking. This class also prepares you for EC-Council ANSI accredited Certified Ethical Hacker certification 312-50.

Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab
* 0 hours externship

Course Objectives

The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation. You walk out the door with ethical hacking skills that are highly in demand, as well as the globally recognized Certified Ethical Hacker certification! This course prepares you for EC-Council Certified Ethical Hacker Certification 312-50

Who Should Attend

This subject is for any individual looking to become a security auditor, security professional, site administrator, and anyone who is concerned about the integrity of the network infrastructure.

Prerequisites

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

Requird Textbooks

EC-Council Digital Courseware 2016

 CEHv9 e-Courseware

Instructional Methods

* Lecture via Remote Live
* Overhead slides
* Cloud-based Lab exercises

Maximum Student to Instructor Ratio

20:1

Outline

**Day 1:**

* Overview of Ethical Hacking
* Footprinting and Recon
* Network Scanning

**Day 2:**

* Enumeration
* System Hacking
* Malware Threats
* Sniffing

**Day 3:**

* Social Engineering
* Denial of Service
* Session Hijacking
* Hijacking Webservers

**Day 4:**

* Hacking Web Apps
* SQL Injection
* Hacking Wireless Networks
* Hacking Mobile Platforms

**Day 5:**

* IDS, Honeypot and Firewall Evasion
* Cloud Computing
* Cryptography
* Penetration Testing

Grading

Grading will be assigned as follows:

* Attendance: 50%
* Lab Assignments: 50%

Subject 312-49: Computer Hacking Forensics Investigator prep

Subject Description

The training in this subject presents a detailed methodological approach to computer forensics and evidence analysis. It is a comprehensive course covering major forensic investigation scenarios that enable you to acquire hands-on experience on various forensic investigation techniques and standard tools necessary to successfully carry-out a computer forensic investigation.

Computer crime in today’s cyber world is on the rise. Computer Investigation techniques are being used by police, government and corporate entities globally. Computer Security and Computer investigations are changing terms. More tools are invented daily for conducting Computer Investigations, be it computer crime, digital forensics, computer investigations, or even standard computer data recovery. The tools and techniques covered in this subject will prepare you to conduct computer investigations using groundbreaking digital forensics technologies.

Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. CHFI investigators can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information known as computer data recovery.

Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab
* 0 hours externship

Course Objectives

When you complete this course, you will be able to understand:

* The process of investigating cybercrime, laws involved, and the details in obtaining a search warrant.
* 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 recover deleted files and deleted partitions in Windows, Mac OS X, and Linux.
* The process involved in forensic investigation using Access Data 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 file breach
* Different types of log capturing techniques, log management, time synchronization and log capturing tools.
* How to investigate logs, network traffic, wireless attacks, and web attacks

Who Should Attend

This course is intended to help you start or advance your career as:

* Computer Forensics Investigators
* Licensed Penetration Tester
* Systems Engineer
* Systems Architect
* Network Security Specialist

RequirEd Textbooks

Certified Hacking Forensic Investigation v9

Course Developer: EC-Council

Author: EC-Council approved SME’s

Publish Date: 2017

Instructional Methods

* Lecture
* Overhead slides
* Cloud-based Lab exercises

Maximum Student to Instructor Ratio

20:1

Outline

**Day 1**

* Computer Forensics in Today’s World
* Computer Forensics Investigation Process
* Searching and Seizing Computers

**Day 2**

* Digital Evidence
* First Responder Procedures
* Computer Forensics Lab
* Understanding Hard Disks and File Systems

**Day 3**

* Windows Forensics
* Data Acquisition and Investigation
* Recovering Deleted Files and Partitions
* Forensics Investigation Using AccessData FTK
* Forensics Investigation Using EnCase

**Day 4**

* Steganography and Image File Forensics
* Application Password Crackers
* Log Capturing and Event Correlation
* Network Forensics, Investigating Logs and Investigating Network Traffic
* Investigating Wireless Attacks

**Day 5**

* Investigating Web Attacks
* Tracking Emails and investigating Email Crimes
* Mobile Forensics
* Investigative Reports
* Becoming an Expert Witness

Grading

Grading will be assigned as follows:

* Attendance: 50%
* Lab Assignments: 50%

Network Support Specialist

Program Description

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

Admission Requirements

Individuals applying for this program are required to:

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

Program Outline

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

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

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00 PM for two weeks, and from 8:00 am to 12:00pm or 1:00pm to 5:00 for two weeks. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For full day students, an hour lunch break will be taken every day from 12:00PM to 1:00PM with four 10 minutes breaks dispersed throughout the day. For morning/afternoon/evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the class.

### Tuition

$12,380

Targeted Job Roles

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

Subject Descriptions

Subject N10-007: CompTIA Network+ Prep

Subject Description

This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network.

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 basic components of network theory.
* Identify the major network communications methods.
* Identify network data delivery methods.
* List and describe network media and hardware components.
* Identify the major types of network implementations.
* Identify the components of a TCP/IP network implementation.
* List the major services deployed on TCP/IP networks.
* Identify characteristics of a variety of network protocols.
* Identify the components of a LAN implementation.
* Identify the components of a WAN implementation.
* Identify major issues and technologies in network security.
* Identify the components of a remote network implementation.
* Identify major issues and technologies in disaster recovery.
* Identify major data storage technologies and implementations.
* Identify the primary network operating systems.
* Identify major issues, models, tools, and techniques in network troubleshooting.

Prerequisites

A typical student taking up the CompTIA® Network+® (N10-007) course should have a minimum of nine months or more of professional computer support experience as a PC or help desk technician. Networking experience is helpful but not mandatory; A+ certification or equivalent skills and knowledge is helpful but not mandatory.

Textbooks / Courseware

CompTIA Network+ N10-007

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 3/3/20

Instructional Methods

* Lecture
* Overhead slides
* Lab

Maximum Student to Instructor Ratio

20:1

Outline

**Day 1:**

**Chapter 1: Security Fundamentals**

* Module A: Security concepts
* Module B: Risk management
* Module C: Vulnerability assessment

**Chapter 2: Understanding attacks**

* Module A: Understanding attackers
* Module B: Social engineering
* Module C: Malware
* Module D: Network attacks
* Module E: Application attacks

**Day 2:**

**Chapter 3: Cryptography**

* Module A: Cryptography concepts
* Module B: Public key infrastructure

**Chapter 4: Network fundamentals**

* Module A: Network components
* Module B: Network addressing
* Module C: Network ports and applications

**Chapter 5: Securing networks**

* Module A: Network security components
* Module B: Transport encryption
* Module C: Hardening networks
* Module D: Monitoring and detection

**Day 3:**

**Chapter 6: Securing hosts and data**

* Module A: Securing hosts
* Module B: Securing data
* Module C: Mobile device security

**Chapter 7: Securing network services**

* Module A: Securing applications
* Module B: Virtual and cloud systems

**Day 4:**

**Chapter 8: Authentication**

* Module A: Authentication factors
* Module B: Authentication protocols

**Chapter 9: Access control**

* Module A: Access control principles
* Module B: Account management

**Day 5:**

**Chapter 10: Organizational security**

* Module A: Security policies
* Module B: User training
* Module C: Physical security and safety

**Chapter 11: Disaster planning and recovery**

* Module A: Business continuity
* Module B: Fault tolerance and recovery
* Module C: Incident response

Grading

Grading will be assigned as follows:

* Attendance: 50%
* Lab Assignments: 50%

#### Subject SY0-601: COMPTIA Security+Prep

##### 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 Prep

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

CISCO Certified Network Associate PREP

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.

Program Objectives

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

You will:

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

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

Program Outline

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

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

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for approximately four weeks. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break.

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

$6,590

Targeted Job Roles

* Network Specialist
* Network Administrators
* Network Support Engineer

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

Technical support specialist

Program Description

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

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

Admission Requirements

Individuals applying for this program are required to:

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

Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| ITIL | ITIL Foundation Certification Prep | 20/20/0/40 |
| 220-1001 | CompTIA A+ Essentials Core 1 Prep | 20/20/0/40 |
| 220-1002 | CompTIA A+ Practical Applications Core 2 Prep | 20/20/0/40 |

The approximate time required to complete this program is five 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 5 days, and from 8:00 am to 12:00 pm or 1:00pm to 5:00 pm for 20 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For full day students, an hour lunch break will be taken every day from 12:00PM to 1:00PM with four 10 minutes breaks dispersed throughout the day. For morning/afternoon/evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

Tuition

$8,085

Targeted Job Roles

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

### Subject Descriptions and Syllabi

#### Subject ITIL: ITIL Foundation certification Prep

##### 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 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%

#### Subject 220-1001: CompTIA A+ ESSENTIALS core 1 PREP

#### Subject Description

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

##### Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab

##### Course Objectives

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

* 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.

##### Who Should Attend

The target student is anyone with basic computer user skills who is interested in obtaining a job as an IT professional or PC technician. Possible job environments include mobile or corporate settings with a high level of face-to face client interaction, remote-based work environments where client interaction, client training, operating systems, and connectivity issues are emphasized, or settings with limited customer interaction where hardware activities are emphasized. In addition, this course will help prepare students to achieve a CompTIA A+ Certification.

##### Prerequisites

Candidates should have the knowledge required to understand the fundamentals of computer technology, networking, and security. They should be able to identify hardware, peripheral, networking, and security components. They should also understand the basic functionality of the operating system and basic troubleshooting methodology.

##### Requird Textbooks

CompTIA A+ Core 1 (220-1001)

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 3/3/2020

##### Instructional Methods

* Lecture
* Overhead slides
* Lab exercises

##### Maximum Student to Instructor Ratio

20:1

##### 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 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

Grading will be assigned as follows:

* Attendance: 50%
* Lab Assignments: 50%

#### Subject 220-1002: CompTIA A+ Practical APPLICATIONS Core 2 PREP

#### Subject 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 Exam

##### Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab

##### Course Objectives

After completing this course, students will be able to:

* 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

##### Prerequisites

Candidates should have the knowledge required to understand the fundamentals of computer technology, networking, and security. They should be able to identify hardware, peripheral, networking, and security components. They should also understand the basic functionality of the operating system and basic troubleshooting methodology.

##### Required Textbooks

CompTIA A+ Core 2 (220-1002)

Course Developer: CompTIA

Authors: James Pengelly

Publish Date 3/3/2020

##### Instructional Methods

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

##### Maximum Student to Instructor Ratio

20:1

#### 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 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.

Information Security Analyst

Program Description

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

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

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

The Information Security Analyst program is available online via Zoom Platform for lectures in which students interact live with faculty. Assessments and Resources (labs, test preps) will be conducted through our Learning Management System online modality. Faculty on a daily basis will take attendance.

##### Course Objectives

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.

The Information Security Analyst program is available online via Zoom Platform for lectures in which students interact live with faculty. Assessments and Resources (labs, test preps) will be conducted through our Learning Management System online modality. Faculty on a daily basis will take attendance.

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.

Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| SY0-601 | CompTIA Security+ Prep | 20/20/0/40 |
| 312-38 | Certified Network Defender Prep | 20/20/0/40 |
| 312-50 | EC-Council Professional Ethical Hacker Prep | 20/20/0/40 |

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

Class Schedule

Day students will attend weekday classes from 8:00AM to 12:00 pm or 1:00 to 5:00 pm for thirty days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

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 morning/afternoon/evening students, there will be no meal time allowed but there will be two 10 minute breaks taken.

Tuition

$10,085

Targeted Job Roles

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

Subject Descriptions

#### Subject SY0-601: COMPTIA Security+Prep

##### 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.

Subject: Certified Network Defender (CND)

Subject Description

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

Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab
* 0 hours externship

Course Objectives

Upon completion of this course, students will expand their Security knowledge and skill on existing topics covered in Security+ and newly introduced topics:

* Security Threats, Vulnerabilities, Attacks
* Network Security Controls
* Network Policy Design
* Physical Security
* Host, Application, Data Security
* Firewalls
* IDS
* VPN
* Wireless Security
* Network Monitoring and Analysis
* Risk and Vulnerability Management
* Data Backup and Recovery
* Network Incident Response

Prerequisites

Security+ or equivalent knowledge

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

Requird Textbooks

CND (Cyber Network Defender)

Author: EC-Council

Publish Date: 2016

#### Instructional Methods

* Lecture
* Overhead slides
* Cloud-based Lab exercises

Maximum Student to Instructor Ratio

20:1

Outline

**Day 1**

* Module 01: Computer Network Defense Fundamentals
* Module 02: Network Security Threats, Vulnerabilities, and Attacks
* Module 03: Network Security Controls, Protocols, and Perimeter Appliances
* Module 04: Secure Firewall Configuration, Deployment and Management

**Day 2**

* Module 05: Secure IDS Configuration and Management
* Module 06: Secure VPN Configuration and Management
* Module 07: Designing a Secure Network
* Module 08: Network Traffic Signatures and Analysis

**Day 3**

* Module 09: Monitoring and Securing Network Traffic
* Module 10: Network Vulnerability Scanning
* Module 11: Monitoring and Securing Network Traffic
* Module 12: Network Vulnerability Scanning

**Day 4**

* Module 13: Host/System Security
* Module 14: Physical Security
* Module 15: Designing and Implementation of Network Security Policies

**Day 5**

* Module 16: Network Incident Response and Management
* Module 17: Network Backup and Disaster Recovery
* Module 18: Wireless Network Defense

Grading

Grading will be assigned as follows:

* Attendance: 50%
* Lab Assignments: 50%

Subject: ec-council certified Professional Ethical Hacker (CEH) prep

Subject 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 leaves this intensive 5 day class, you will have hands on understanding and experience in Ethical Hacking. This class also prepares you for EC-Council ANSI accredited Certified Ethical Hacker Certification 312-50.

Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab
* 0 hours externship

Course Objectives

The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation. You walk out the door with ethical hacking skills that are highly in demand, as well as the globally recognized Certified Ethical Hacker certification! This course prepares you for EC-Council Certified Ethical Hacker Certification 312-50.

Prerequisites

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

Requird Textbooks

Certified Ethical Hacker v10

Course Developer: EC-Council

Author: EC-Council approved SME’s

Publish Date: 2018

Instructional Methods

* Lecture
* Overhead slides
* Cloud-based Lab exercises

Maximum Student to Instructor Ratio

20:1

Outline

**Day 1:**

* Overview of Ethical Hacking
* Footprinting and Recon
* Network Scanning

**Day 2:**

* Enumeration
* System Hacking
* Malware Threats
* Sniffing

**Day 3:**

* Social Engineering
* Denial of Service
* Session Hijacking
* Hijacking Webservers

**Day 4:**

* Hacking Web Apps
* SQL Injection
* Hacking Wireless Networks
* Hacking Mobile Platforms

**Day 5:**

* IDS, Honeypot and Firewall Evasion
* Cloud Computing
* Cryptography
* Penetration Testing

Grading

Grading will be assigned as follows:

* Attendance: 50%
* Lab Assignments: 50%

CompTIA NETWORK+ prep

### Program Description

CompTIA Network+ is a short certification program geared specifically towards entry-level jobs in IT networking, such as Network Technician & Network Support.

Course Objectives

This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network.

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

* Identify the basic components of network theory.
* Identify the major network communications methods.
* Identify network data delivery methods.
* List and describe network media and hardware components.
* Identify the major types of network implementations.
* Identify the components of a TCP/IP network implementation.
* List the major services deployed on TCP/IP networks.
* Identify characteristics of a variety of network protocols.
* Identify the components of a LAN implementation.
* Identify the components of a WAN implementation.
* Identify major issues and technologies in network security.
* Identify the components of a remote network implementation.
* Identify major issues and technologies in disaster recovery.
* Identify major data storage technologies and implementations.
* Identify the primary network operating systems.
* Identify major issues, models, tools, and techniques in network troubleshooting.

### 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

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| N10-007 | CompTIA Network+ Prep | 20/20/0/40 |

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

### Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00 PM for 5 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For full day students, an hour lunch break will be taken every day from 12:00PM to 1:00PM with four 10 minutes breaks dispersed throughout the day. For morning/afternoon/evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

### Tuition

$2,895

### Targeted Job Roles

* Network Support
* Network Technician
* Network Operating Center Analyst
* Network Support Specialist

### Subject Descriptions

#### Subject N10-007: CompTIA Network+ Prep

##### Subject Description

This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network.

##### 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 basic components of network theory.
* Identify the major network communications methods.
* Identify network data delivery methods.
* List and describe network media and hardware components.
* Identify the major types of network implementations.
* Identify the components of a TCP/IP network implementation.
* List the major services deployed on TCP/IP networks.
* Identify characteristics of a variety of network protocols.
* Identify the components of a LAN implementation.
* Identify the components of a WAN implementation.
* Identify major issues and technologies in network security.
* Identify the components of a remote network implementation.
* Identify major issues and technologies in disaster recovery.
* Identify major data storage technologies and implementations.
* Identify the primary network operating systems.
* Identify major issues, models, tools, and techniques in network troubleshooting.

##### Prerequisites

A typical student taking up the CompTIA Network+ course should have nine months or more of professional computer support experience. Networking experience is helpful but not mandatory; A+ certification or equivalent skills and knowledge is helpful but not mandatory.

##### Textbooks / Courseware

CompTIA Network+ N10-007

Course Developer: CompTIA

Authors: James Pengelly

Publish Date: 3/3/20

##### Instructional Methods

* Lecture
* Overhead slides
* Lab

##### 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%
* Lab Assignments: 50%

CompTIA Security+ prep

### Program Description

CompTIA Security+ is a short certification program geared specifically towards entry level jobs in IT security, such as IT Security Analyst & Computer Support Specialist. After taking this course, students will understand the field of network security and how it relates to other areas of information technology.

### 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

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| SY0-601 | CompTIA Security+ Prep | 20/20/0/40 |

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

### Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00 PM for 5 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For full day students, an hour lunch break will be taken every day from 12:00PM to 1:00PM with four 10 minutes breaks dispersed throughout the day. For morning/afternoon/evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

### Tuition

$2,895

### Targeted Job Roles

* IT Security Analyst
* Computer Support Specialist
* Network Support Specialist

### Subject Descriptions

#### Subject SY0-601: COMPTIA Security+Prep

##### 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.

EC-COUNCIL CERTIFIED ETHICAL HACKER prep - (CEH)

PROGRAM DESCRIPTION

The Certified Ethical Hacker program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

This class will immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be led into scanning and attacking their own networks. No real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system.

Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this intensive 5-day program course they will have hands-on understanding and experience in Ethical Hacking.

COURSE OBJECTIVES

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

After completing the program, students will be able to:

* Perform ethical hacking for vulnerability assessments, and
* Accurately report on their findings.

Targeted Job Roles

* Ethical Hackers
* Security Consultants
* IT Managers
* Chief Security Officers

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.

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| 312-50 | EC-COUNCIL Certified Ethical Hacker (CEH) Prep | 20/20/0/40 |

PREREQUISITES

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

Tuition

$3,795

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00 PM for 5 days. Classes Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For full day students, an hour lunch break will be taken every day from 12:00PM to 1:00PM with four 10 minutes breaks dispersed throughout the day. For morning/afternoon/evening students, there will be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

PROGRAM hours

40 hours total:

* 20 hours lecture
* 20 hours lab
* 0 hours externship

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

REQUIRED TEXTBOOK

Certified Ethical Hacker v10

Course Developer: EC-Council

Author : EC-Council approved SME’s

Published Date: 2018

INSTRUCTIONAL METHODS

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

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM OUTLINE

Day 1

* Security Fundamentals
* Access Controls
* Protocols

Day 2

* Cryptography
* Why Vulnerability Assessments
* Vulnerability Tools of the Trade

Day 3

* Output Analysis and Reports
* Reconnaissance, Enumeration and Scanning

Day 4

* Gaining Access
* Maintaining Access
* Covering Tracks

Day 5

* Malware
* Buffer Overflows
* Password Cracking

GRADING

Grading will be assigned as follows:

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

CERTIFIED NETWORK DEFENDER prep- (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.

COURSE OBJECTIVES

Students will learn:

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

Targeted Job Roles

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

Admission Requirements

Individuals applying for this program are required to:

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

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| 312.-38 | Certified Network Defender (CND) PREP | 20/20/0/40 |

PREREQUISITES

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

Tuition

$3,795

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 5 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For day students, an hour lunch break will be taken every day from 11:30PM 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 hours

40 hours total:

* 20 hours lecture
* 20 hours lab
* 0 hours externship

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

REQUIRED TEXTBOOK

Certified Network Defender

Course Developer: EC-Council

Author EC-Council approved SME’s

Publish Date: 2017

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Lab Exercises

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

Outline

**Day 1**

* Module 01: Computer Network Defense Fundamentals
* Module 02: Network Security Threats, Vulnerabilities, and Attacks
* Module 03: Network Security Controls, Protocols, and Perimeter Appliances
* Module 04: Secure Firewall Configuration, Deployment and Management

**Day 2**

* Module 05: Secure IDS Configuration and Management
* Module 06: Secure VPN Configuration and Management
* Module 07: Designing a Secure Network
* Module 08: Network Traffic Signatures and Analysis

**Day 3**

* Module 09: Monitoring and Securing Network Traffic
* Module 10: Network Vulnerability Scanning
* Module 11: Monitoring and Securing Network Traffic
* Module 12: Network Vulnerability Scanning

**Day 4**

* Module 13: Host/System Security
* Module 14: Physical Security
* Module 15: Designing and Implementation of Network Security Policies

**Day 5**

* Module 16: Network Incident Response and Management
* Module 17: Network Backup and Disaster Recovery
* Module 18: Wireless Network Defense

Grading

Grading will be assigned as follows:

* Attendance: 50%
* Lab Assignments: 50%

COMPUTER HACKING FORENSIC INVESTIGATOR prep - (CHFI)

PROGRAM DESCRIPTION

The EC-Council 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.

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

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

COURSE OBJECTIVES

Students will learn:

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

Targeted Job Roles

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

Admission Requirements

Individuals applying for this program are required to:

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

Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours** |
| 312-49 | COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI) PREP | 20/20/0/40 |

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 knowledge and experience

Tuition   
$3,795

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 5 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For day students, an hour lunch break will be taken every day from 11:30PM 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.

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

REQUIRED TEXTBOOK

Certified Hacking Forensic Investigation v9

Course Developer: EC-Council

Author: EC-Council approved SME’s

Publish Date: 2017

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Lab Exercises

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

Outline

**Day 1**

* Computer Forensics in Today’s World
* Computer Forensics Investigation Process
* Searching and Seizing Computers

**Day 2**

* Digital Evidence
* First Responder Procedures
* Computer Forensics Lab
* Understanding Hard Disks and File Systems

**Day 3**

* Windows Forensics
* Data Acquisition and Investigation
* Recovering Deleted Files and Partitions
* Forensics Investigation Using AccessData FTK
* Forensics Investigation Using EnCase

**Day 4**

* Steganography and Image File Forensics
* Application Password Crackers
* Log Capturing and Event Correlation
* Network Forensics, Investigating Logs and Investigating Network Traffic
* Investigating Wireless Attacks

**Day 5**

* Investigating Web Attacks
* Tracking Emails and investigating Email Crimes
* Mobile Forensics
* Investigative Reports
* Becoming an Expert Witness

Grading

Grading will be assigned as follows:

* Attendance: 50%
* Lab Assignments: 50%

EC-COUNCIL CERTIFIED ENCRYPTION SPECIALIST prep-(ECES)

PROGRAM DESCRIPTION

If you think that there is only one type of encryption – think again! Secure organizations employ multiple levels of encryption – database encryption, VoIP encryption, portable storage encryption, mobile devices encryption, Wi-Fi encryption, e-mail encryption, file encryption – server/desktop, network link encryption, web server encryption, tape backup encryption and many more.

Some of the most recent attacks that have had serious consequences share one thing in common – they all had either little or no effective encryption. This resulted in thousands of users being affected and hundreds of millions in losses. It resulted in serious decline of brand value and public embarrassment. And these were not technically naïve companies by any means. To name a few – SONY PS3, RSA, iPhone, LinkedIn.

The ECES course introduces students to modern symmetric key cryptography including the details of algorithms such as Feistel Networks, DES, and AES as well as an overview of many other algorithms such as Blowfish, Twofish, Skipjack, and others. Other topic areas include the basics of information theory as it applies to cryptography; an introduction to hashing algorithms including MD5, MD6, SHA, Gost, RIPMD 256 and others; asymmetric cryptography including thorough descriptions of RSA, Elgamal, Elliptic Curve, and DSA; significant concepts such as diffusion, confusion, and Kerkcho’s principle.

COURSE OBJECTIVES

Students will learn:

* The basics of information theory as it applies to cryptography.
* An introduction to hashing algorithms including MD5, MD6, SHA, Gost, RIPMD 256 and others.
* Asymmetric cryptography including thorough descriptions of RSA, Elgamal, Elliptic Curve, and DSA.
* Significant concepts such as diffusion, confusion, and Kerkcho’s principle.
* Types of encryption standards and their differences.
* How to select the best standard for your organization.
* How to enhance your pen-testing knowledge in encryption.
* Correct and incorrect deployment of encryption technologies.
* Common mistakes made in implementing encryption technologies.
* Best practices when implementing encryption technologies.

Targeted Job Roles

* Entry Level Penetration Testers
* Junior Computer Forensic Specialists
* Anyone involved in basic information security operations

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.

Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours** |
| 212-81 | EC-COUNCIL CERTIFIED ENCRYPTION SPECIALIST (ECES) PREP | 12/12/0/24 |

PREREQUISITES

* Basic computer literacy
* Basic PC Operating System navigation skills
* Basic Internet usage skills
* Basic IP addressing knowledge
* No prior knowledge of cryptography is assumed, and no mathematical skills beyond basic algebra are required.

Tuition

$2,545

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 3 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For day students, an hour lunch break will be taken every day from 11:30PM 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 hours

24 hours total:

* 24 hours lecture
* 0 hours labs
* 0 hours externship

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

REQUIRED TEXTBOOK

Certified Encryption Specialist Vol. 1  
EC-Council Official Courseware

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM OUTLINE

**CORE MODULES**

**Day 1:**

* Introduction and History of Cryptography
* Symmetric Cryptography & Hashes

**Day 2:**

* Number Theory and Asymmetric Cryptography
* Applications of Cryptography

**Day 3:**

* Cryptanalysis

GRADING

Grading will be assigned as follows:

* Attendance: 50%
* Participation: 50%

COMPTIA ADVANCED SECURITY PRACTITIONER prep- (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 on these subject matter areas as they relate to the CASP certification objectives.

COURSE 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 (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.

PREREQUISITES

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

Tuition

$3,495

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 5 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For day students, an hour lunch break will be taken every day from 11:30PM 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

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours** |
| CASP-002 | CompTIA Advanced Security Practitioner Prep | 20/20/0/40 |

The approximate time required to complete this program is five days for day students and 10 evenings for evening 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%

Itil foundations Certification prep

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. ITIL stands for IT Infrastructure Library.

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.

Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| ITIL | ITIL Foundation Certification Prep | 20/20/0/40 |

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

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 5 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For day students, an hour lunch break will be taken every day from 11:30PM 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

$3,495

Targeted Job Roles

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

### Subject Descriptions and Syllabi

#### Subject ITIL: ITIL Foundation Certification Prep

##### 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 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 3-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

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 Completion

##### Grading

Grading will be assigned as follows:

* Attendance: 75%
* Exercise Participation: 25%

## Comptia a+ certification prep

PROGRAM DESCRIPTION

The CompTIA A+ 1001 course will build on your existing user-level knowledge and experience with personal computer (PC) hardware to present fundamental skills and concepts that you will use on the job. In this course, you will acquire the essential skills and information you will need to install, configure, troubleshoot, upgrade, and perform preventive maintenance on PCs and mobile device hardware.

The CompTIA A+ (220-1001) course can benefit you in two ways. Whether you work or plan to work in a mobile or corporate environment where you have 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 you will require to be a successful A+ technician.

The 1002 course will build on your existing user-level knowledge and experience with personal computer (PC) software and operating systems to present fundamental skills and concepts that you will use on the job. In this course, you will acquire the essential skills and information you will need to install, configure, optimize, troubleshoot, upgrade, secure, and perform preventive maintenance on PC and digital device operating systems.

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

Course Objectives

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

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.

Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| 220-1001 | CompTIA A+ Essentials Core 1 Prep | 20/20/0/40 |
| 220-1002 | CompTIA A+ Practical Applications Core 2 Prep | 20/20/0/40 |

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

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 10 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For day students, an hour lunch break will be taken every day from 11:30PM 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

$5,790

Targeted Job Roles

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

### Subject Descriptions and Syllabi

#### Subject 220-1001: CompTIA A+ Essentials Prep

##### Subject Description

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

##### Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab

##### Course Objectives

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

* 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.

##### Who Should Attend

The target student is anyone with basic computer user skills who is interested in obtaining a job as an IT professional or PC technician. Possible job environments include mobile or corporate settings with a high level of face-to face client interaction, remote-based work environments where client interaction, client training, operating systems, and connectivity issues are emphasized, or settings with limited customer interaction where hardware activities are emphasized. In addition, this course will help prepare students to achieve a CompTIA A+ Certification.

##### Prerequisites

Candidates should have the knowledge required to understand the fundamentals of computer technology, networking, and security. They should be able to identify hardware, peripheral, networking, and security components. They should also understand the basic functionality of the operating system and basic troubleshooting methodology.

##### Requird Textbooks

CompTIA A+ Core 1 (220-1001)

Course Developer: CompTIA

Authors: James Pengelly

Publish Date 3/3/20

##### Instructional Methods

* Lecture
* Overhead slides
* Lab exercises

##### Maximum Student to Instructor Ratio

20:1

##### 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 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

* Grading will be assigned as follows:
* 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.

#### Subject 220-1002: CompTIA A+ Practical APPLICATIONS Core 2 PREP

##### Subject Description

* 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.

##### Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab

##### Course Objectives

After completing this course, students will be able to:

* 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
* Prerequisites

Candidates should have the knowledge required to understand the fundamentals of computer technology, networking, and security. They should be able to identify hardware, peripheral, networking, and security components. They should also understand the basic functionality of the operating system and basic troubleshooting methodology.

##### Required Textbooks

CompTIA A+ Core 2 (220-1002)

Course Developer: CompTIA

Authors: James Pengelly

Publish Date 3/3/20

##### Instructional Methods

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

##### Maximum Student to Instructor Ratio

20:1

#### 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 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

Grading will be assigned as follows:

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.

Senior technology Project MANAGER - (STPM)

### 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.

### Course Objective

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

* Understand the philosophy of modern project management
* Prepare a Project Charter
* Conduct a stakeholder analysis
* Create a work breakdown structure for a project
* Develop a project schedule using the critical path method
* Apply basic risk management on a project
* Prepare a communications plan for a project
* Manage project changes and risk events
* Integrate the basic functions of project management throughout a project life cycle.
* Understand the key concepts of ITIL
* Apply principles for improving IT operations and project success
* Provide practical guidance for applying ITIL to everyday IT project situations
* Understand how to align with business, control costs, and improve IT service quality
* Implement strategies to balance IT resources
* Identify personal strengths and weaknesses in each of the knowledge areas
* Explain the correct answers to each of the sample exam questions
* Develop a personalized strategy for passing the PMP Exam

### Admission Requirements

Individuals applying for this program are required to have a bachelor’s degree and 4,500 hours of Project Management experience in the five PM process groups, OR, a secondary school diploma and 7,500 hours of PM experience in the five process groups.

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| ITIL | ITIL Foundation Certification Prep | 20/20/0/40 |
| CAPM/PMP | CAPM /PMP IT Project manager Prep | 40/0/0/40 |

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

### Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 10 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For day students, an hour lunch break will be taken every day from 11:30PM 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.

ll be no meal time allowed but there will be two 10 minute breaks taken throughout the evening.

Tuition

$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-FND: ITIL Foundation Certification Prep

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

##### Prerequisites:

There are no prerequisites.

##### 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

REQUIRED TEXTBOOK

ITIL 4 Foundation

Course Developer: Logical Operations

Authors: Patrick Von Schlag ITIL Expert

Laurie Perry

Publish Date2019

#### CAPM/PMP- Project Management Professional Prep

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.

PERFORMANCE OBJECTIVES

Students will learn:

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

Targeted Job Roles

* Project Managers

Admission Requirements

Individuals applying for this program are required to:

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

PREREQUISITES

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

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.

REQUIRED TEXTBOOK

Project Management Body of Knowledge (PMBOK Guide) v6

Course Developer: Project Management Institute (PMI)

Author:Project Management Institute (PMI)

Publish Date: 2017

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

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 PMP
* 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%

## CAPM & PMP IT project manager Prep

##### 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.

##### Course Objective

Students will learn:

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

Targeted Job Roles

* Project Managers

Admission Requirements

Individuals applying for this program are required to:

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

##### Prerequisites

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

Tuition

$3,295

Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 10 days. Classes for evening students will be held Monday through Friday 6:00pm – 10:00pm, 7:00pm -11:00pm or 8:00pm - 12:00am Some Saturdays allowed for make-up 8:00am – 5:00pm with one hour lunch break

For day students, an hour lunch break will be taken every day from 11:30PM 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

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours** |
| CAPM/PMP | CAPM/Project Management Professional Prep | 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 Body of Knowledge (PMBOK Guide) v6

Course Developer: Project Management Institute (PMI)

Author:Project Management Institute (PMI)

Publish Date: 2017

INSTRUCTIONAL METHODS

* Lecture
* Overhead slides
* Labs

MAXIMUM STUDENT TO INSTRUCTOR RATIO

20:1

PROGRAM OUTLINE

**Day 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

**Day 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

**Day 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

**Day 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

**Day 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%

Certified Information Systems Security Professional prep- (CISSP)

### Program Description

This Program is for individuals who plan to build a career in information security - one of today's most visible professions. The Certified Information System Security Professional Certification is for IS security professionals who develop policies and procedures in information security.

The Certified Information System Security Professional was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Organization for Standardization) Standard 17024:2003.

The Certified Information System Security Professional program demonstrates competence in the ten domains of the ISC2 Certified Information System Security Professional CBK. The ten domains are as follows:

* Access Control
* Application Development Security
* Business Continuity and Disaster Recovery Planning
* Cryptography
* Information Security Governance and Risk Management
* Legal, Regulations, Investigations and Compliance
* Operations Security
* Physical (Environmental) Security
* Security Architecture and Design
* Telecommunications and Network Security

### 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

### Program Outline

|  |  |  |
| --- | --- | --- |
| **Course Number** | **Course Title** | **Clock Hours Lecture/Lab/Ext/Total** |
| CISSP | Certified Information Systems Security Professional Prep | 20/20/0/40 |

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

### Class Schedule

Day students will attend classes Monday through Friday from 8:00AM to 5:00PM for 5 days. Classes for evening students will be held Mondays through Friday from 7:00PM to 11:00PM. For day students, an hour lunch break will be taken every day from 11:30PM 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

$3,495.00

### Targeted Job Roles

* IT Security Analyst
* IT Compliance Specialist
* IT Auditor
* Information Security Manager

### Subject Descriptions

#### Subject: Certified Information System Security Professional

##### The Certified Information Systems Security Professional certification is a globally recognized standard of achievement that verifies an individual’s knowledge in the field of information security. Certified Information System Security Professional are information assurance professionals who define the architecture, design, management and/or controls that assure the security of business environments.

##### Subject Hours

40 hours total:

* 20 hours lecture
* 20 hours lab

##### Course Objectives

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

* Analyze information systems access control.
* Analyze security architecture and design.
* Analyze network security systems and telecommunications.
* Analyze information security management goals.
* Analyze information security classification and program development.
* Analyze risk management criteria and ethical codes of conduct.
* Analyze software development security.
* Analyze cryptography characteristics and elements.
* Analyze physical security.
* Analyze operations security.
* Apply Business Continuity and Disaster Recovery Plans.
* Identify legal issues, regulations, compliance standards, and investigation practices relating to information systems security.

##### Textbooks / Courseware

CISSP 5th Edition

Course Developer: Logical Operations/ISC2

Author Chrys Thorsen, Jason Nufryk

##### Publish Date: 2018

##### Instructional Methods

* Lecture
* Overhead slides
* Lab

##### Maximum Student to Instructor Ratio

20:1

##### Outline

**Day 1**

Lesson 1: Information Systems Access Control

* Topic 1A: Data Access Principles
* Topic 1B: System Access and Authentication
* Topic 1C: Attacks and Penetration Tests

Lesson 2: Security Architecture and Design

* Topic 2A: Security Architecture Frameworks and Security Models
* Topic 2B: Security Modes
* Topic 2C: System Assurance

**Day 2**

Lesson 3: Network and Telecommunications Security

* Topic 3A: Data Network Design
* Topic 3B: Remote Data Access
* Topic 3C: Data Network Security
* Topic 3D: Data Network Management

Lesson 4: Information Security Management Goals

* Topic 4A: Organizational Security
* Topic 4B: The Application of Security Concepts

**Day 3**

Lesson 5: Information Security Classification and Program Development

* Topic 5A: Information Classification
* Topic 5B: Security Program Development

Lesson 6: Risk Management and Ethics

* Topic 6A: Risk Management
* Topic 6B: Ethics

Lesson 7: Software Development Security

* Topic 7A: Software Configuration Management
* Topic 7B: Software Controls
* Topic 7C: Database System Security

**Day 4**

Lesson 8: Cryptography

* Topic 8A: Ciphers and Cryptography
* Topic 8B: Symmetric-Key Cryptography
* Topic 8C: Asymmetric-Key Cryptography
* Topic 8D: Hashing and Message Digests
* Topic 8E: Email, Internet, and Wireless Security
* Topic 8F: Cryptographic Weaknesses

Lesson 9: Physical Security

* Topic 9A: Physical Access Control
* Topic 9B: Physical Access Monitoring
* Topic 9C: Physical Security Methods
* Topic 9D: Facilities Security

Lesson 10: Operations Security

* Topic 10A: Operations Security Control
* Topic 10B: Operations Security Auditing and Monitoring
* Topic 10C: Operational Threats and Violations

**Day 5**

Lesson 11: Business Continuity and Disaster Recovery Planning

* Topic 11A: Business Continuity Plan Fundamentals
* Topic 11B: Business Continuity Plan Implementation
* Topic 11C: Disaster Recovery Plan Fundamentals
* Topic 11D: Disaster Recovery Plan Implementation

Lesson 12: Legal, Regulations, Compliance, and Investigations

* Topic 12A: Computer Crime Laws and Regulations
* Topic 12B: Computer Crime Incident Response

#### Grading

Grading will be assigned as follows:

* Attendance: 50%
* Lab Assignments: 50%