DoD TRAINING CENTER
YOU CAN SLEEP WHEN YOU'RE CERTIFIED

COURSE CATALOGUE

January 2022 – December 2022 Catalogue

DoD Training Center
January 2022

Site Administrator: **Pierre Colombel**

Columbia MD: 8830 Standford Blvd, Ste 100, Columbia, MD 21045

E-mail: pierre@dodtc.com

Phone: (443) 841-9890

CAGE Code: 5NF42 / DUNS: 786455746

Fed Tax ID: 22-3956137

Site Administrator: **Raymond Hughes**

San Diego CA: 9089 Clairemont Mesa Blvd, Ste 110, San diego, CA 92123

E-mail: Raymond.Hughes@dodtc.com

Phone: (858) 215-6174

CAGE Code: 8KUJ4 / DUNS: 100440728

Fed Tax ID: 84-4061575

Included with each seat are:	Covid Safety Measures:
- 5 days of instruction **- Exam voucher** **- Course materials** **- Courseware** **- Books** **- Exam prep tests** **- Testing and Proctor on final day of class** **- Pass guarantee or retest onsite**	**- Mask required for all trainees** **- Classroom: 15 Max** **- Class area limited to only course attendees** **- Desk cleaned w/ disinfectant** **- 3x Daily - Before Class** ** - During Class** ** - After Class** **- Temperature check daily**

Site Staff

Pierre Colombel – DoD Training Center – Columbia Maryland

CEO / Site Director / Instructor

Certificatoins: Microsoft Certified Trainer (MCT) • CISSP, CISM • PMP • CompTIA A+, Network+, Security+, CASP • MCITP Windows 7, MCITP Enterprise Administrator • MCSE + Security 2003, • MCTS SQL 2005, • MCTS SharePoint • MCTS Virtualization (Hyper-V), • EC-Council Certified Ethical Hacker (CEH) • EC-Council Certified Security Analyst (E-CSA) • EC-Council (LPT) Licensed Penetration Tester• CHF • CIH • CCISO RMF & eMASS • ISSAP • ISSEP.

Raymond Hughes – DoD Training Center – San Diego California

CIO / Site Director / Instructor

Certificatoins: CISSP • CISM • EC-Council Certified Ethical Hacker (CEH) • EC-Council Certified Network Defense Architect (CNDA) • CompTIA A+, Network+, Security+, CYSA, CASP, Project+.

Student Policies

Definitions:

 i) 'The Training Center' – DoD Training Center and sub-sites, training locations, and online classroom.

ii) 'The Candidate or Student' – the person who is attending a course or bootcamp.

iii) 'Organization' – entity administratively or professional responsible for the candidates attending a course.

iv) 'Fee payer' – person responsible for the payment of fees. Hereafter the 'Fee Payer' may be a US Government Entity, DoD Entity, Corporate Entity, or an individual.

 v) 'Training Course' – A bootcamp, class, lab or course of instruction in a particular specialty.

Admission: Candidate enrollment is on a per seat basis. Organizations or individuals who wish to attend a training course may submit enrollment request via one of several methods: E-mail, Phone, or site registration. Candidates will receive a quote via FreshBooks for the requested seat(s) in the desired course(s) which may chose ala cart. Candidates are enrolled and place onto a class roster once payment has been made for the requested courses.

Course Completion: Training courses are usually presented in bootcamp format but may be longer based on requests from the requesting organization. Bootcamps are 5 days long either Monday thru Friday (8:30am – 5pm) or 5 consecutive weekends in accordance with scheduled meeting times. Candidates must attend 90% or more of the 40 hour class to be credited with attending the full course. Candidates will receive a course completion certificate at the end of the course. Certification is dependent on candidates successfully passing the certification exam.

Testing and Certification: Candidates must score an 800 on the final practice exam to be allowed to take the official certification exam. Candidates may take the certification exam in class on the final day, at an authorized test center, or online. Certification exam scores vary by certification and organization. However, candidates must achieve a score high enough to meet the minimum pass requirement for the certification being taken to receive that certification. Practice exam results are presented to students in the practice exam software. Candidates will receive a Certification Exam Score Report for the official certification exam taken.

Candidate Conduct: Candidates are to conduct themselves in an orderly and ethical manner as not to disturb other students or tenants of the training center. Candidates may bring personal laptops, cell phones, PDA or other electronic devices. Candidates will be given WiFi access, however, are not permitted to physically connect their personal devices to any portion or physical asset on the training center network. Candidates will be given access to sharable resources. Candidates may not attempt to copy, reduplicate, reproduce, or divulge any portion of the official certification exam contents. Candidates must agree to follow the test proctor's / test centers explicit instructions during any testing period.

Tuition and Fees: Tuition is paid as quoted per seat. Payment must be made within 1 week before course start for individuals and 2 weeks before course start for organizations.

Refunds: Course tuition is refundable up to 2 weeks before course start. After this period tuition is NOT refundable. However, candidates may request to attend the course on different dates. Candidates must provide prior notification in the case of absence due to unforeseen circumstances or changes to attendance dates. FAILURE to do so will result in FULL FORFITURE of the course tuition.

Support Services: Candidates will receive instructor support from the date of registration for a course through the end of the course and certification test. Instructors will make themselves available before and after class and during breaks for additional assistance with course material and concepts. Instructors are available for questions from 8am to 10pm.

Job Support: DoD Training Center does not provide job placement; however, enjoys many relationships with various industry partners and IT talent scouts. DoD Training center will share those contact resources with candidates and provide limited introductions.

1. **CompTIA**
   a. A+
   b. Network +
   c. Security +
   d. Cloud +
   e. CySA +
   f. CASP +
2. Microsoft
   a. Azure
   b. Dynamics 365
   c. Exchange Server
   d. PowerShell
   e. SharePoint Server
   f. SQL Server
   g. System Center
   h. Visual Studio
   i. Windows Server
3. **EC-Council**
   a. CEH
   b. ECSA
   c. EDRP
   d. CHFI
   e. C|CISO
4. ISACA
   a. CISA
   b. CISM
   c. CRISC
5. CISCO
   a. CCNA
   b. CCNP Routing and Switching
   c. CCNA Security
   d. CCENT
   e. CCDA

6. VMWare
   a. VMware Certified Associate (VCA)
   b. VMware Certified Professional (VCP)
   c. VMware Certified Advanced Professional (VCAP)
   d. VMware Certified Design Expert (VCDX)
7. ITIL
   a. ITIL 4 Foundation Training.
   b. ITIL 4 Managing Professional Transition Training.

c. ITIL 4 Specialist: Create, Deliver and Support.

    d. ITIL 4 Specialist: Drive Stakeholder Value.

    e. ITIL 4 Specialist: Hi Velocity IT.

    f. ITIL 4 Strategist: Direct, Plan and Improve.

    g. ITIL 4 Leader: Digital and IT Strategy.

8. AWS

    a. AWS Certified Cloud Practitioner.

    b. AWS Certified Developer – Associate.

    c. AWS Certified SysOps Administrator – Associate.

    d. AWS Certified Solutions Architect – Associate (SAA-C02)

    e. AWS Certified DevOps Engineer – Professional.

    f. AWS Certified Solutions Architect – Professional

9. Citrix

    a. Citrix Certified Associate – Networking

    b. Citrix Certified Professional – Networking

10. RED HAT

    a. RHCSA I

    b. RHCSA II

    c. RHCE

11. Splunk

    a. Splunk Users

    b. Splunk Administrators

    c. Advanced Splunk

12. Python

COURSE

CompTIA A+

Description section:

Course overview

Held by over 1 million IT professionals worldwide, CompTIA A+ is the most essential IT certification for establishing an IT career. If you're new to the IT industry, this will help you put your best foot forward. And if you're already an IT professional, the CompTIA A+ certification validates your skills and can boost your career.

A+ is comprehensive and vendor-neutral
A+ certified professionals have mastered the technologies found in today's extensive and varied IT environments, from mobile to traditional devices and operating systems. They can confidently handle the most challenging technology problems more efficiently.

A+ validates foundational skills
A+ establishes best practices in troubleshooting, networking and security across a variety of devices to set the stage for IT careers. The certification also matches professional tech skills with communication skills.

A+ is trusted by employers

As businesses and governments worldwide continue to adopt mobile and cloud technology, they trust A+ certified professionals to keep their devices running and organizations working smoothly.

A+ is globally recognized and accredited

CompTIA A+ is compliant with ISO 17024 standards and is approved by the U.S. Department of Defense to meet directive 8140/8570.01-M requirements.

A+ is industry supported

A+ is developed and maintained by leading IT experts. Content for the exams stems from a combination of industry-wide survey feedback and contributions from our team of subject matter experts.

WHAT YOU'LL LEARN

- Prepare for the latest A+ certification exams (CompTIA A Plus Certification Prep)
- Fundamentals of computer technology
- Install and configure PC operating systems
- Configure common features for Android and Apple iOS mobile operating systems
- PC components
- Preventative maintenance
- Operating system technologies
- Communicate with customers in a professional manner
- Computer hardware and peripherals
- Network connections
- Laptop and portable computing device components
- Support printers and scanners
- Secure PCs

WHATS INCLUDED:

- All Courseware
- Hands on labs with real equipment
- Tool Kit
- Practice exams
- Exam Vouchers required to pass the exam

PREREQUISITES

- End-user skills with Windows-based PCs

- Basic knowledge of computing concepts

WHO SHOULD ATTEND

- Information Technology (IT) professionals who have networking and administrative responsibilities.

- Anyone who wants to further their career in IT by acquiring foundational knowledge of security topics.

- Candidates for S+ certification

Follow up CourSes:

Network+ Microsoft/Cisco. Ask your Rep to map out a career path.

CERTIFICATIONS:

Attain A+ certification by passing 220-801 and 220-802 exams

OUTLINE & LABS

1. Troubleshooting

- Troubleshooting theory

- Safety

2. Motherboards and CPUs

- Motherboards
- CPUs

3. Computer Power Supplies

- Power supply connectors
- Power supply installation
- Power supply troubleshooting

4. Memory

- Read-only memory
- Random access memory

5. Computer Expansion

- Expansion interfaces
- Expansion card installation
- Connectors and cables

6. Physical Storage

- Disk drives
- Redundant array of independent disks (RAID)
- Optical drives
- Other storage methods

7. Input-Output Devices

- Input devices
- Output devices
- Dual input-output devices

8. Display Devices

- Display types
- Display installation
- Display troubleshooting

9. Operating Systems

- Windows versions and features
- Windows installation and upgrades
- Non-Windows operating systems

   10. Windows Management

- Operating system features and tools
- Control Panel utilities
- Command-line tools
- Troubleshooting

   11. Network Basics

- Classifying networks
- Network devices
- Internet connections

   12. Network Cables and Connectors

- Twisted-pair connections
- Coaxial connections
- Optical media

   13. Network Protocols

- TCP/IP settings
- Transport protocols
- Application protocols

   14. Wireless Networking

- Wi-Fi standards
- Wireless encryption

   15. Windows Networking

- Sharing and security
- Network connections
- Connection troubleshooting

   16. Virtualization and Cloud Computing

- Virtualization

- Cloud computing

17. Mobile Devices

- Mobile device types
- Mobile device connectivity
- Mobile device troubleshooting

18. Security Basics

- Security threats
- Threat prevention

19. Securing Devices and Data

- Workstation security
- Mobile device security
- Security troubleshooting

20. SOHO Network Configuration

- SOHO router features
- Network security

21. Printers and Multifunction Print Devices

- Printer technologies
- Printer installation
- Printer maintenance
- Printer troubleshooting

22. Custom Computers

- Custom computer considerations

23. Operational Procedures

- Environment
- Safety
- Content and privacy

NETWORK +

Description section:

Course overview

Earning CompTIA's Network+ certification increases your value in the marketplace by providing proof of your knowledge, skills, and ability to manage, maintain, troubleshoot, install, operate, and configure a basic network infrastructure. Our Network+ Prep Course allows you to demonstrate the concepts covered on the Network+ exam using a sophisticated remote lab environment. Work through several practice exams to reinforce your knowledge and gain essential networking skills in labs featuring networking devices such as routers, switches, access points, and others. As an added bonus, you may access the practice exam on your own computer. (CompTIA Network Plus)

WHAT YOU'LL LEARN

- Prepare for the CompTIA Network+ certification exam (N10-006) (Network Plus)
- Basic network theory concepts
- Industry standard communications methods
- Network media and hardware components
- Components of a TCP/IP network implementation

- TCP/IP addressing and data delivery methods

- Crucial services employed in TCP/IP network environments

- Components of local area networks (LANs)

- Wide area network (WAN) concepts and associated technologies

- Components of remote network implementation

- Major issues and methods to secure systems on a network

- Major issues and technologies in network security

- Network security threats and attacks

- Tools, methods, and techniques used in managing a network

- Troubleshooting network issues

WHATS INCLUDED:

- All Courseware
- Hands on labs with real equipment
- Tool Kit
- Practice exams
- Exam Vouchers required to pass the exam

PREREQUISITES

COMPTIA RECOMMENDS (BUT DOES NOT REQUIRE) 9 MONTHS OF NETWORK-RELATED IT EXPERIENCE.

WHO SHOULD ATTEND

- IT personnel who need a solid foundation in networking

- Individuals interested in pursuing the CompTIA Network+ certification exam N10-006

- Managers and supervisors who must oversee network-related activities.

Follow up Courses:

There are many options following this course. Ask your Rep to map out potential next steps.

CERTIFICATIONS:

NETWORK+

OUTLINE & LABS

1. Network Media and Devices

- Topologies and the OSI Model
- Cabling and Connectors
- Ethernet
- Bridge and Switches

2. Addressing and Routing

- Internet Protocol
- Addressing Schemes
- DHCP and APIPA
- IPv6
- Routing

3. Network Applications

- Transport Protocols
- Name Resolution
- Web Services
- Communication Services
- WAN Technologies

- Remote Access

4. Network Security

- Security Fundamentals

- Security Appliances

- Authentication

- Installing Wireless Networks

5. Management, Monitoring, Troubleshooting

- Configuration Management

- Installing Wired Networks

- Deploying Virtual Networks

- Monitoring and Management Tools

- Network Troubleshooting

    - Lab 1: Configuring a Network Adapter
    - Lab 2: Using Hyper-V
    - Lab 3: ARP and Packet Analysis
    - Lab 4: IP Address Configuration
    - Lab 5: IP Addressing Schemes
    - Lab 6: Configuring DHCP in Windows
    - Lab 7: Configuring DHCP in Linux
    - Lab 8: IPv6 Addressing
    - Lab 9: Configuring Routing
    - Lab 10: TCP and Port Scanning
    - Lab 11: Name Resolution
    - Lab 12: Configuring DNS
    - Lab 13: Configuring Email Services
    - Lab 14: Performance Testing and Monitoring

  - Lab 15: Monitoring and Management Tools

OUTLINE & LABS

Module 1: Security Fundamentals

- The Information Security Cycle

- Information Security Controls

- Authentication Methods

- Cryptography Fundamentals

- Security Policy Fundamentals

Module 2: Identifying Security Threats and Vulnerabilities
- Social Engineering

- Malware

- Software-Based Threats

- Network-Based Threats

- Wireless Threats and Vulnerabilities

- Physical Threats and Vulnerabilities

Module 3: Managing Data, Application, and Host Security
- Data Security

- Application Security

- Device and Host Security

SECURITY+

Course overview

CompTIA® Security+® (Exam SY0-401) is the primary training course you will need to take if your job responsibilities include securing network services, devices, and traffic in your organization. You can also take this course to prepare for the CompTIA Security+ certification examination. 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+ (Exam SY0-401) certification examination, this course can be a significant part of your preparation. But 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.

WHAT YOU'LL LEARN

- Identify the fundamental concepts of computer security

- Identify security threats and vulnerabilities

- Manage data, application, and host security

- Implement network security

- Identify and implement access control and account management security measures

- Manage certificates

- Identify and implement compliance and operational security measures

- Manage risk

- Troubleshoot and manage security incidents

- Plan for business continuity and disaster recovery

What's Included

- All Courseware

- Practice exams via Portal

- Optional Evening Review Sessions in addition to the 5 days of training

- Pre/Post Assessments

- S+ Exam Voucher

PREREQUISITES

- CompTIA A+ and Network+ certifications, or equivalent knowledge

- Six to nine months experience in networking including configuring security parameters

WHO SHOULD ATTEND

- Information Technology (IT) professionals who have networking and administrative responsibilities.

- Anyone who wants to further their career in IT by acquiring foundational knowledge of security topics.

- Candidates for S+ certification

OUTLINE & LABS

Module 1: Security Fundamentals
- The Information Security Cycle

- Information Security Controls

- Authentication Methods

- Cryptography Fundamentals

- Security Policy Fundamentals

Module 2: Identifying Security Threats and Vulnerabilities
- Social Engineering

- Malware

- Software-Based Threats

- Network-Based Threats

- Wireless Threats and Vulnerabilities

- Physical Threats and Vulnerabilities

Module 3: Managing Data, Application, and Host Security
- Data Security

- Application Security

- Device and Host Security

- Mobile Security

Module 4: Implementing Network Security
- Configure Security Parameters on Network Devices and Technologies

- Network Design Elements and Components

- Implement Networking Protocols and Services

- Apply Secure Network Administration Principles

- Secure Wireless Traffic

Module 5: Implementing Access Control, Authentication, and Account Management
- Access Control and Authentication Services

- Implement Account Management Security Controls

Module 6: Managing Certificates
- Install a CA Hierarchy

- Enroll Certificates

- Secure Network Traffic by Using Certificates

- Renew Certificates

- Back Up and Restore Certificates and Private Keys

- Revoke Certificates

Module 7: Implementing Compliance and Operational Security
- Physical Security

- Legal Compliance

- Security Awareness and Training

- Integrate Systems and Data with Third Parties

Module 8: Risk Management
- Risk Analysis

- Implement Vulnerability Assessment Tools and Techniques

- Scan for Vulnerabilities

- Mitigation and Deterrent Techniques

Module 9: Troubleshooting and Managing Security Incidents
- Respond to Security Incidents

- Recover from a Security Incident

Module 10: Business Continuity and Disaster Recovery Planning
- Business Continuity

- Plan for Disaster Recovery

- Execute DRPs and Procedures

CompTIA Cloud +

Description section:

 Course overview

As more and more businesses shift their IT operations to cloud platforms, skills in cloud computing and virtualization have become a frequently required qualification for IT professionals. Cloud+ is globally recognized and accredited. CompTIA Cloud+ is compliant with ISO 17024 standards. Adding CompTIA Cloud+ to your resume demonstrates your ability to implement and maintain cloud technologies and enables you to jump into a rapidly growing market:

- 9 out of 10 companies use some form of cloud technology[1].
- 60 percent of companies have 30 percent or more of their IT systems in the cloud[1].
- Cloud computing is estimated to generate nearly 7 million jobs worldwide by the end of 2015[2].
- The global cloud computing market is projected to reach $270 billion by 2020[1].

 WHAT YOU'LL LEARN

- Cloud concepts, models, and terminology

- Systems management

- Storage networking

- Disk storage systems

- Virtualization and the cloud

- Performance tuning

- Systems management

- Testing and troubleshooting

- Cloud security

- Business continuity and disaster recovery

   The Cloud+ certification exam objectives are as follows:

- Cloud Concepts and Models (12%)

- Virtualization (19%)

- Infrastructure (21%)

- Resource Management (13%)

- Security (16%)

- Systems Management (11%)

- Business Continuity in the Cloud (8%)

WHATS INCLUDED:

- All Courseware
- Practice exams
- Exam Vouchers required to pass the exam

PREREQUISITES

2-3 YEARS OF HANDS-ON INFORMATION SECURITY OR RELATED EXPERIENCE, SECURITY + AND OR NETWORK+ RECOMMENDED.

WHO SHOULD ATTEND

- Cloud Specialists
- Network Engineers
- Cloud Sales Executives
- Cloud Developers
- Network Architects
- Infrastructure Engineers for Government Programs
- Government Sector Solutions Architects
- Network, Storage, Systems and Data Center Administrators

OUTLINE & LABS

1. Threat Management
   1. Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes.
   2. Given a scenario, analyze the results of a network reconnaissance.
   3. Given a network-based threat, implement or recommend the appropriate response and countermeasure
   4. Explain the purpose of practices used to secure a corporate environment.

2. Vulnerability Management
   1. Given a scenario, implement an information security vulnerability management process.
   2. Given a scenario, analyze the output resulting from a vulnerability scan
   3. Compare and contrast common vulnerabilities found in the following targets within an organization.

3. Cyber Incident Response
   1. Given a scenario, distinguish threat data or behavior to determine the impact of an incident.
   2. Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation
   3. Explain the importance of communication during the incident response process
   4. Given a scenario, analyze common symptoms to select the best course of action to support incident response
   5. Summarize the incident recovery and post-incident response process

4. Security Architecture and Tool Sets

1. Explain the relationship between frameworks, common policies, controls, and procedures

    2. Given a scenario, use data to recommend remediation of security issues related to identity and access management.

    3. Given a scenario, review security architecture and make recommendations to implement compensating controls.

    4. Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC)

    5. Compare and contrast the general purpose and reasons for using various cybersecurity tools and technology.

COMPTIA CYBERSECURITY ANALYST (CYSA+)

Description section:

Course overview

As attackers have learned to evade traditional signature-based solutions such as firewalls, an analytics-based approach within the IT security industry is increasingly important for most organizations. The behavioral analytics skills covered by CSA+ identify and combat malware, and advanced persistent threats (APTs), resulting in enhanced threat visibility across a broad attack surface

WHAT YOU'LL LEARN

- Configure and use threat detection tools.
- Perform data analysis.
- Interpret the results to identify vulnerabilities, threats and risks to an organization.

WHATS INCLUDED:

- All Courseware
- Practice exams
- Exam Vouchers required to pass the exam

PREREQUISITES

  3-4 YEARS OF HANDS-ON INFORMATION SECURITY OR RELATED EXPERIENCE, SECURITY + AND OR NETWORK+ RECOMMENDED.

WHO SHOULD ATTEND

- The CompTIA Cybersecurity Analyst (CSA+) examination is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts. The exam will certify that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization.

 OUTLINE & LABS

1. Threat Management
    6. Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes
    7. Given a scenario, analyze the results of a network reconnaissance
    8. Given a network-based threat, implement or recommend the appropriate response and countermeasure
    9. Explain the purpose of practices used to secure a corporate environment
2. Vulnerability Management
    1. Given a scenario, implement an information security vulnerability management process
    2. Given a scenario, analyze the output resulting from a vulnerability scan

3. Compare and contrast common vulnerabilities found in the following targets within an organization

3. Cyber Incident Response

1. Given a scenario, distinguish threat data or behavior to determine the impact of an incident.

2. Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation

3. Explain the importance of communication during the incident response process

4. Given a scenario, analyze common symptoms to select the best course of action to support incident response

5. Summarize the incident recovery and post-incident response process

2. Security Architecture and Tool Sets

1. Explain the relationship between frameworks, common policies, controls, and procedures

2. Given a scenario, use data to recommend remediation of security issues related to identity and access management

3. Given a scenario, review security architecture and make recommendations to implement compensating controls

4. Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC)

5. Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies

CompTIA Advanced Security Practitioner (CASP) Prep Course

Description section:

 Course overview

You have experience in the increasingly crucial field of information security, and now you're ready to take that experience to the next level. CompTIA® Advanced Security Practitioner (CASP) (Exam CAS-002) is the course you will need to take if your job responsibilities include securing complex enterprise environments. In this course, you will expand on your knowledge of information security to apply more advanced principles that will keep your organization safe from the many ways it can be threatened. Today's IT climate demands individuals with demonstrable skills, and the information and activities in this course can help you develop the skill set you need to confidently perform your duties as an advanced security professional. This course is designed for IT professionals who want to acquire the technical knowledge and skills needed to conceptualize, engineer, integrate, and implement secure solutions across complex enterprise environments.

This course can also benefit you if you intend to pass the CompTIA Advanced Security Practitioner (CAS-002) certification examination. What you learn and practice in this course can be a significant part of your preparation

WHAT YOU'LL 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

WHATS INCLUDED:

- All Courseware
- Practice exams
- Exam Vouchers required to pass the exam

PREREQUISITES

INTERNETWORKING WITH TCP/IP AND SWITCHING IN IP NETWORKS IS STRONGLY RECOMMENDED

WHO SHOULD ATTEND

- Individuals seeking the CompTIA Advanced Security Practitioner (CASP) certification (Exam CAS-002)

- IT professionals with a minimum of 10 years of experience in IT administration and at least five years of hands-on security in an enterprise environment

FOLLOW UP COURSES:

There are many options following this course like CEH and CISM. Ask your Rep to map out potential next steps.

CERTIFICATIONS:

COMPTIA ADVANCED SECURITY PRACTITIONER (CASP) CAS-003

OUTLINE & LABS

- Managing Risk
- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

  2. INTEGRATING COMPUTING, COMMUNICATIONS, AND BUSINESS DISCIPLINES

- Facilitate Collaboration Across Business Units
- Secure Communications and Collaboration Solutions
- Implement Security Activities Throughout the Technology Life Cycle

  3. USING RESEARCH AND ANALYSIS TO SECURE THE ENTERPRISE

- Determine Industry Trends and Effects on the Enterprise
- Analyze Scenarios to Secure the Enterprise

  4. INTEGRATING ADVANCED AUTHENTICATION AND AUTHORIZATION TECHNIQUES

- Implement Authentication and Authorization Technologies
- Implement Advanced Identity Management

  5. IMPLEMENTING CRYPTOGRAPHIC TECHNIQUES

- Describe Cryptographic Concepts
- Choose Cryptographic Techniques
- Choose Cryptographic Implementations

6. IMPLEMENTING SECURITY CONTROLS FOR HOSTS

- Select Host Hardware and Software
- Harden Hosts
- Virtualize Servers and Desktops
- Implement Cloud Augmented Security Services
- Protect Boot Loaders

7. IMPLEMENTING SECURITY CONTROLS FOR ENTERPRISE STORAGE

- Identify Storage Types and Protocols
- Implement Secure Storage Controls

8. ANALYZING AND IMPLEMENTING NETWORK SECURITY

- Analyze Network Security Components and Devices
- Analyze Network-Enabled Devices
- Analyze Advanced Network Design
- Configure Controls for Network Security

9. IMPLEMENTING SECURITY CONTROLS FOR APPLICATIONS

- Identify General Application Vulnerabilities
- Identify Web Application Vulnerabilities
- Implement Application Security Controls

10. INTEGRATING HOSTS, STORAGE, NETWORKS, AND APPLICATIONS IN A SECURE ENTERPRISE ARCHITECTURE

- Implement Security Standards in the Enterprise
- Select Technical Deployment Models
- Secure the Design of the Enterprise Infrastructure
- Secure Enterprise Application Integration Enablers

11. CONDUCTING VULNERABILITY ASSESSMENTS

- Select Vulnerability Assessment Methods
- Select Vulnerability Assessment Tools

12. RESPONDING TO AND RECOVERING FROM INCIDENTS

- Design Systems to Facilitate Incident Response

- Conduct Incident and Emergency Responses

  CLASSROOM LIVE LABS
  LAB 1: INTEGRATE DOCUMENTATION INTO RISK MANAGEMENT

  LAB 2: SECURE COMMUNICATIONS AND COLLABORATION SOLUTIONS

  LAB 3: ANALYZE SCENARIOS TO SECURE THE ENTERPRISE

  LAB 4: IMPLEMENT AUTHENTICATION AND AUTHORIZATION TECHNOLOGIES

  LAB 5; CHOOSE CRYPTOGRAPHIC TECHNIQUES

  LAB 6: HARDEN HOSTS

  LAB 7: VIRTUALIZE SERVERS AND DESKTOPS

  LAB 8: PROTECT BOOT LOADERS

  LAB 9: IMPLEMENT SECURE STORAGE CONTROLS

  LAB 10: CONFIGURE CONTROLS FOR NETWORK SECURITY

  LAB 11: IMPLEMENT APPLICATION SECURITY CONTROLS

  LAB 12: SELECT VULNERABILITY ASSESSMENT TOOLS

  LAB 13: DESIGN SYSTEMS TO FACILITATE INCIDENT RESPONSE

  LAB 14: CONDUCT INCIDENT AND EMERGENCY RESPONSES

IMPLEMENTING MICROSOFT AZURE INFRASTRUCTURE SOLUTIONS (20533)

Description section:

Course overview:

In this course, you will learn the architecture, services, tools, and portals of Microsoft Azure. You will take your knowledge and experience in System Center, Windows Server, and Windows Development to the cloud by learning how to manage and implement virtual networking in Azure, implementing websites and data services, Azure Content Delivery Networks, and create and manage Azure Active Directory.

This course incorporates materials from the Official Microsoft Learning Product 20533 and it can assist you in your preparation for Exam 70-533: Implementing Microsoft Azure Infrastructure Solutions.

Ask About Digital learning if time & budget is an issue.

WHAT YOU'LL LEARN

- Azure architecture components including infrastructure, tools, and portals
- Implement and manage virtual networking within Azure and connecting to on-premise environments
- Plan and create Azure virtual machines
- Optimize availability and reliability for Azure virtual machines
- Implement, manage, back up, and monitor storage solutions
- Plan and implement data services based on structured query language (SQL) databases to support applications
- Deploy and configure websites
- Publish content through Azure Content Delivery Networks
- Create and manage Azure AD Directories
- Integrate on-premises Windows AD with Azure AD
- Automate operations in Azure management by using PowerShell runbooks

PREREQUISITES

- Network configuration including TCP/IP, DNS, virtual private networks (VPNs), firewalls, and encryption technologies
- Creating, configuring, deploying, and monitoring a website on IIS
- Active Directory concepts including domains, forests, domain controllers, replication, Kerberos, and LDAP
- Database concepts including tables, queries, SQL, database replication, and database schemas Resilience and disaster recovery including backup and restoration, operations, and clustering

- Familiarity with Windows PowerShell

 WHO SHOULD ATTEND

- IT Professionals
- Server Administrators
- Windows Server Administrators
- Developers

Follow Up Courses: Check with your Rep for advice on next steps.

Certifications: MCSA Cloud Platform & MCSE Cloud Platform and Infrastructure

OUTLINE

VIRTUAL CLASSROOM LIVE OUTLINE
1Introduction to Azure

- Cloud Technology Overview
- Azure Infrastructure Review
- Azure Portals
- Managing Azure Using Windows PowerShell
- Overview of Azure Resource Manager

2. Implement and Manage Azure Networks

- Plan Virtual Networks
- Implement and Manage Azure Virtual Networks
- Configure Connections to Azure Virtual Networks

3. Implement Virtual Machines

- Overview of Azure Resource Manager virtual machines

- Planning for Azure virtual machines

- Deploying Azure Resource Manager virtual machines

- Authoring Azure Resource Manager templates

  4. Overview of classic virtual machines Manage Virtual Machines

- Configure Virtual Machines

- Manage and Configure Virtual Machine Disks

- Manage and Monitor Azure Virtual Machines

  5. Implement Azure App services

- Plan for App Deployment in App Service

- Deploy, Configure, and Monitor Web Apps

- Traffic Manager

  6. Plan and Implement Storage, Backup, and Recovery Services

- Plan, Implement, and Manage Storage

- Implement Azure Content Delivery Networks

- Implementing Azure Backup and Azure Site Recovery

  7. Plan and Implement Azure SQL Database

- Deploy Azure SQL Database

- Monitor Azure SQL Database

- Manage Azure SQL Database Security and Azure SQL Database Business Continuity

  8. Implement PaaS Cloud Services

- Plan and Deploy PaaS Cloud Services

- Configure Remote Desktop Protocol (RDP)

- Monitoring Cloud Services

  9. Implement Azure Active Directory (AD)

- Create and Manage Azure AD tenants

- Configure Application Integration with Azure AD

- Overview of Azure AD Premium

  10. Manage AD in the Hybrid Environment

- Extend On-Premises Active Directory Deployments into Azure

- Directory Synchronization

- Implement Federation

11. Implement Azure-based Management and Automation

- Implement Microsoft Operations Management Suite (OMS)
- Automation Components
- PowerShell WorkflowsManaging Automation

CLASSROOM LIVE LABS

Note: Given the dynamic nature of Microsoft cloud tools, you may experience changes in the interface that do not match up with courseware. Your DoDTC instructor will always teach to the latest release, and guide you through the updates as needed.

Lab 1: Managing Microsoft Azure

- Navigate the Portals
- Install and Use Windows Azure PowerShell

Lab 2: Use a Deployment Template to Implement Azure Virtual Networks

- Create and the Virtual Network by using PowerShell
- Configure Virtual Networks

Lab 3: Configure Connectivity between classic and Azure Resource Manager virtual networks

- Use a PowerShell Script to connect a classic VNet and an Azure Resource Manager VNet
- Configure a Point-To-Site VPN
- Validate virutal network connectivity

Lab 4: Create and Azure Resource Manager virtual machines in Azure

- Creating Virtual Machines by using the Azure Portal and Azure PowerShell
- Validate virtual machine creation

Lab 5: Deploy Azure Resource Manager virtual machines by using Azure Resource Manager templates

- Use Visual Studio and an Azure Resource Manager template to deploy virtual machines
- Use Azure PowerShell and an Azure Resource Manager template to deploy virtual machines

Lab 6: Manage Azure Virtual Machines

- Configure Virtual Machine Storage
- Implement Desired State Configuration (DSC)
- Implement Storage Space-Based Volumes

Lab 7: Implement Websites

- Create, Deploy, and Manage a Web Apps

- Implement Traffic Manager

  Lab 8: Plan and Implement Storage

- Create and Configure Storage

- Azure File Storage

- Protect Data with Azure Backup

  Lab 9: Plan and Implement Azure SQL Database

- Create, Secure, and Monitor an Azure SQL Database

- Migrate a Database to Azure SQL Database

- Restore a Database

  Lab 10: Implement PaaS Cloud Services

- Deploy a Cloud Service

- Configure Deployment Slots and Remote Desktop Protocol

- Monitor Cloud Services

  Lab 11: Implement Azure Active Directory

- Administer AD

- Configure Single Sign-On

- Configure Multi-Factor Authentication

  Lab 12: Implement and Manage an Azure AD Synchronization

- Configure Directory Synchronization

- Synchronize Directories

  Lab 13: Implement Automation

- Configure Automation Accounts

- Create Runbooks

ENABLING AND MANAGING OFFICE 365

Course overview:

In this 5-day course, you will learn to evaluate, plan, deploy, and operate Microsoft Office 365 services, including its identities, dependencies, requirements, and supporting technologies. You will learn the skills required to set up and sustain an Office 365 tenant and users.

Ask About Digital learning if time & budget is an issue.

WHAT YOU'LL LEARN

- Plan an Office 365 deployment, configure the Office 365 tenant, and plan a pilot deployment
- Manage Office 365 users, groups, and licenses, and configure delegated administration
- Plan and configure client connectivity to Office 365
- Plan and configure directory synchronization between Azure AD and on-premises AD DS
- Plan and implement the deployment of Office 365 ProPlus
- Plan and manage Exchange Online recipients and permissions
- Plan and configure Exchange Online services
- Plan and implement the Skype for Business Online deployment
- Plan and configure SharePoint Online
- Plan and configure an Office 365 collaboration solution that includes Yammer Enterprise, OneDrive for Business, and Office 365 groups
- Plan and configure the integration between Office 365 and Azure RMS, and configure compliance features in Office 365
- Monitor and review Office 365 services, and troubleshoot Office 365 issues
- Plan and implement identity federation between on-premises AD DS and Azure AD

This course comes with 12 months access to the following benefits:

- Practice Labs
- 24x7 Mentoring
- Indexed Class Recordings
- Unlimited Retakes
- Digital Courseware

PREREQUISITES

- Cloud-based service concepts
- Overview of Office 365 and its component services
- Active Directory Service
- TCP/IP network routing

- Domain Name Services (DNS)

- X.509 Certificates

- Firewall ports

-

- IT professionals who evaluate, plan, deploy, and operate Microsoft Office 365 services including its dependencies, requirements, and supporting technologies

- Network administrators and IT managers responsible for managing and maintaining Office 365, including identities, document protection, integration with on-premise directory services, and compliance with service level agreements.

Certifications:

MCSA Office 365

MCSE Productivity

FOLLOW ON CLASSES: **PLANNING FOR AND MANAGING DEVICES IN THE ENTERPRISE - ENTERPRISE MOBILITY SUITE AND ON-PREMISES TOOLS (20398)**

OUTLINE

1. Planning and Provisioning Microsoft Office 365 Introduction to Office 365

- Overview of Office 365

- Provisioning an Office 365 tenant

- Planning a pilot deployment

2. Managing Microsoft Office 365 Users and groups

- Managing user accounts and licenses

- Managing passwords and authentication

- Managing security groups in Office 365

- Managing Office 365 users and groups with Windows PowerShell
- Configuring administrative access

3. Configuring Client Connectivity to Microsoft Office 365

- Planning for Office 365 clients
- Planning connectivity for Office 365 clients
- Configuring connectivity for Office 365 clients

4. Planning and Configuring Directory Synchronization

- Planning and preparing for directory synchronization
- Implementing directory synchronization by using Azure Active Directory (AD) Connect
- Managing Office 365 identities with directory synchronization

5. Planning and Deploying Office 2016 ProPlus

- Overview of Office 365 ProPlus
- Planning and managing user-driven Office 365 ProPlus deployments
- Planning and managing centralized deployments of Office 365 ProPlus
- Office telemetry and reporting

6. Planning and Managing Exchange Online Recipients and Permissions

- Overview of Exchange Online
- Managing Exchange Online recipients
- Planning and configuring Exchange Online permissions

7. Planning and Configuring Microsoft Exchange Online Services

- Planning and configuring email flow in Office 365
- Planning and configuring email protection in Office 365
- Planning and configuring client access policies
- Migrating to Exchange Online

8. Planning and Deploying Skype for Business Online

- Planning and configuring Skype for Business Online service settings
- Configuring Skype for Business Online users and client connectivity
- Planning voice integration with Skype for Business Online

9. Planning and Configuring SharePoint Online

- Configuring SharePoint Online services

- Planning and configuring SharePoint site collections
- Planning and configuring external user sharing

10. Planning and Configuring an Office 365 Collaboration Solution

- Planning and managing Yammer Enterprise
- Planning and configuring OneDrive for Business
- Configuring Office 365 groups

11. Planning and Configuring Rights Management and Compliance

- Overview of the compliance features in Office 365
- Planning and configuring Azure Rights Management in Office 365
- Managing the compliance features in Office 365

12. Monitoring and Troubleshooting Microsoft Office 365

- Troubleshooting Office 365
- Monitoring Office 365 service health

13. Planning and Configuring Identity Federation

- Identity federation
- Planning an Active Directory Federation Services (AD FS) deployment
- Deploy AD FS for identity federation with Office 365

LABS

CLASSROOM LIVE LABS
Note: Given the dynamic nature of Microsoft cloud tools, you may experience changes in the interface that do not match up with courseware. Your Global Knowledge instructor will teach to the latest release, and guide you through the updates as needed.

Lab 1: Provisioning Office 365

- Configuring an Office 365 tenant
- Configuring a custom domain
- Exploring the Office 365 administrator interfaces

Lab 2: Managing Office 365 Users and Passwords

- Managing Office 365 users and licenses by using the Office 365 admin center
- Managing Office 365 password policies

Lab 3: Managing Office 365 Groups and Administration

- Managing Office 365 groups
- Managing Office 365 users and groups by using Windows PowerShell
- Configuring delegated administrators

  Lab 4: Configuring Client Connectivity to Office 365

- Configuring DNS records for Office 365 clients
- Running the Office 365 connectivity analyzer tools
- Connecting Office 2016 clients

  Lab 5: Planning and Configuring Directory Synchronization

- Preparing for directory synchronization
- Configuring directory synchronization
- Managing Active Directory users and groups

  Lab 6: Deploying Office 365 ProPlus

- Preparing an Office 365 ProPlus managed installation
- Managing user-driven Office 365 ProPlus installations
- Managing Centralized Office 365 ProPlus installations

  Lab 7: Managing Exchange Online Recipients and Permissions

- Configuring Exchange Online recipients
- Configuring delegated administration

  Lab 8: Configuring Message Transport in Exchange Online

  Lab 9: Configuring Email Protection and Client Policies

- Configuring email protection
- Configuring client access policies

  Lab 10: Deploying Skype for Business Online

- Configuring Skype for Business Online organization settings
- Configuring Skype for Business Online user settings
- Configuring a Skype Meeting Broadcast

  Lab 11: Configuring SharePoint Online

- Configuring SharePoint Online settings

- Creating and configuring a SharePoint Online site collection
- Configuring and verifying external user sharing

Lab 12: Planning and Configuring an Office 365 Collaboration Solution

- Configuring a Yammer Enterprise
- Configuring OneDrive for Business
- Configuring Office 365 groups

Lab 13: Configuring Rights Management and Compliance

- Configuring rights management in Office 365
- Configuring compliance features

Lab 14: Monitoring and Troubleshooting Office 365

- Monitoring Office 365
- Monitoring service health and analyzing reports

Lab 15: Planning and Configuring Identity Federation

- Deploying AD FS and Web Application
- Configuring federation with Office 365
- Verifying single sign-on (SSO)

Microsoft:

AUTOMATING ADMINISTRATION WITH WINDOWS POWERSHELL
Updated – Learn to remotely manage your Windows-based servers with PowerShell.

Description section:

Course overview:

In this 5-day course, you will gain the fundamental knowledge and skills to use Windows PowerShell for administering and automating the administration of your Windows-based servers. You will focus on primary Windows PowerShell command line features and techniques. You will gain prerequisite skills that support different Microsoft products. Learn to execute and monitor scripts more efficiently with more robust session connectivity, workflow capabilities, improved job scheduling, and Windows PowerShell Web Access.

This course incorporates materials from the Official Microsoft Learning Product M10961: Automating Administration with Windows PowerShell.

Ask About Digital learning if time & budget is an issue.

WHAT YOU'LL LEARN

- Basic concepts behind Windows PowerShell

- Work with the Pipeline

- How the Pipeline works

- Use PSProviders and PSDrives

- Format output

- Use Windows Management Instrumentation (WMI) and Common Information Model (CIM)

- Prepare for scripting

- Moving from a command to a script to a module

- Administer remote computers

- Put the various Windows PowerShell components together

- Use background jobs and scheduled jobs

- Use advanced PowerShell techniques and profiles

This course comes with 12 months access to the following benefits:

- Practice Labs

- 24x7 Mentoring

- Indexed Class Recordings

- Unlimited Retakes

- Digital Courseware

PREREQUISITES

- Previous Windows Server and Windows Client management knowledge and hands-on experience

- Experience installing and configuring Windows Server into existing enterprise environments, or as standalone installations

- Knowledge and experience of network adapter configuration, basic Active Directory user administration, and basic disk configuration

- Knowledge and hands-on experience specifically with Windows Server 2012 and Windows 8 would be beneficial

- IT Professionals already experienced in general Windows Server and Windows Client administration or already experienced in administering and supporting application servers and services, including Exchange, SharePoint, SQL, etc.
- Students who want to use Windows PowerShell to automate administrative tasks from the command line, using any Microsoft or independent software vendor (ISV) product that supports Windows PowerShell manageability

Follow on Classes: **Core Solutions of Microsoft Exchange Server 2013 (20341)**

Certifications: None

OUTLINE

Windows PowerShell

- Overview and Background
- Finding and Running Commands

Cmdlets for administration

- Active Directory administration cmdlets
- Network configuration cmdlets
- Other server administration cmdlets

Working with the Windows PowerShell Pipeline

- Selecting, Sorting, and Measuring Objects
- Exporting, Importing, and Converting Data
- Filtering Objects Out of the Pipeline
- Enumerating Objects in the Pipeline

How the Pipeline Works

- Passing the Pipeline Data

- Advanced Considerations for Pipeline Data

Using PSProviders and PSDrives

- PSProviders and PSDrives

Querying System Information Using WMI and CIM

- Querying Data with WMI/CIM
- Making Changes with WMI/CIM

Working with Variables, Arrays, and Hash Tables

- Using Variables
- Manipulating Arrays and Hash Tables

Basic Scripting

- Introduction to Scripting
- Scripting Constructs
- Importing Data from Files

Advanced Scripting

- Accepting User Input
- Overview of Script Documentation
- Troubleshooting and Error Handling
- Functions and Modules

Administering Remote Computers

- Using Basic Windows PowerShell Remoting
- Using PSSessions
- Using Advanced Remoting Techniques

Using Background Jobs and Scheduled Jobs

- Using Background Jobs
- Using Scheduled Jobs

Using Advanced PowerShell Techniques and Profiles

- Using Advanced PowerShell Techniques
- Creating Profile Scripts

LABS

Configure Windows PowerShell

- Configure the Console Application

- Configure the ISE Application

Find and Run Basic Commands

- Finding commands

- Running commands

- Using the About files

Windows Administration

- Creating and managing Active Directory objects

- Configuring network settings on Windows Server

- Creating a web site

Use the Pipeline

- Select and Sort Data

Filtering Objects

Enumerating Objects

Sending Output to a File

- Exporting user information to a file

Work with Pipeline Parameter Binding

- Predict Pipeline Behavior

Use PSProviders and PSDrives

- Create a new folder on a remote computer

- Create a registry key for future scripts

- Create a new Active Directory group

- Work with WMI and CIM

- Locate and query information with WMI and CIM

Working with Variables

- Working with variable types

- Using arrays

- Using hash tables
- Using hash tables

Basic Scripting

- Setting a script
- Processing an array with a ForEach loop
- Processing items by using If statements
- Creating a random password
- Creating users based on a CSV file

Accepting Data from Users

- Querying disk information from remote computers
- Updating the script to use alternate credentials
- Documenting a script

Implementing Functions and Modules

- Creating a logging function
- Adding error handling to a script
- Converting a function to a module

Using Basic Remoting

- Enabling remoting on the local computer
- Performing one-to-one remoting
- Performing one-to-many remoting

Using PSSessions

- Using implicit remoting
- Managing multiple computers

Using Background Jobs and Scheduled Jobs

- Starting and managing jobs
- Creating a scheduled job

Practicing Advanced Techniques

- Creating a profile script
- Verifying the validity of an IP address
- Reporting disk information

- Configuring NTFS permissions
- Creating user accounts with passwords from a CSV file

Course 55255-A: SharePoint for Office 365 End User Training

Description section:

Course overview:

This three-day instructor-led SharePoint for Office 365 End User Training class is for end users and site owners/managers new to working in a SharePoint environment in Office 365. The course teaches SharePoint basics such as working with lists and libraries, basic page customization, working with forms and managing site permissions and users.

Ask About Digital learning if time & budget is an issue.

WHAT YOU'LL LEARN

Navigate a SharePoint Team Site.

Create SharePoint lists.

Customize SharePoint lists.

Create SharePoint libraries.

Manage library document versions.

Create SharePoint list and library views.

Create sub sites using various SharePoint templates.

Create and edit Web page content.

Create InfoPath Forms and Form libraries.

Create Site columns and content types.

Integrate Office applications with SharePoint.

Manage basic permissions of SharePoint resources

PREREQUISITES

- Understanding of networking fundamentals
- Experience configuring security and administration tasks in an enterprise environment
- Experience supporting or configuring Windows Client with Windows Vista, Windows 7, or Windows 8

-

WHO SHOULD ATTEND

This course is intended for new and existing users of SharePoint. This course is for information workers.

OUTLINE

- Module 1: SharePoint 365 Setup
- This module explains how to set up SharePoint 365.
- Lessons
- SharePoint Online
- After completing this module, students will be able to:
- Set up the sample site for class.
- Module 2: SharePoint 365 Introduction
- SharePoint 365 is a collaboration tool at its heart. Its primary goal is to make it easy for users to find and share information, and there are many features built into SharePoint

to facilitate this. SharePoint's library system feature can provide a superior alternative to the traditional file server. SharePoint lists can be an easy-to-design and easy-to-use alternative to sharing spreadsheet files or more formal database tables. Both lists and libraries can be customized and extended to provide enhanced appearances and functionality. All of this collaboration can be done through a browser interface.

-
- Lessons
- SharePoint Online
- Site Layout and Navigation
- Layout
- Navigation
- Lab : Team Site Navigation
- After completing this module, students will be able to:
-
- Learn abbout SharePoint online.
- Learn about SharePoint site hierarchy.
- Module 3: SharePoint List Basics
- Lists are a fundamental building block in SharePoint that provides a way for users to store and view data. SharePoint comes "out of the box" with many predefined list templates that are easy to use. Lists can be further customized by adding columns to store just about any type of information. Additionally, list columns can be validated as well as linked between other lists. Lists are a very flexible and powerful tool in SharePoint.
-
- Lessons
- Creating Apps Using List Templates
- Creating Lists
- Creating Lists Using List Templates
- List Columns
- Creating List Columns
- Column Validation
- Validating a List Column
- Lab : Working with Team Site Lists
- Lab : Create Custom Lists and Columns

- After completing this module, students will be able to:

-

- Work with List Templates.

- Work with default lists in a Team Site.

- Create a new list from a List Template.

- Create a custom list.

- Add columns to a list.

- Control and validate input into list fields.

- Link data from separate lists

- Module 4: Library Basics

- SharePoint Libraries share the same characteristics as SharePoint lists such as columns, views, and validation to name a few. What distinguishes SharePoint libraries is that each item in a library has an underlying document. So in addition to the data stored in library columns, the document stores its own data based on the type of document. Because of the extra data that can be stored in columns that can be used to filter and search by and features such as versioning, libraries are considered a great replacement for the more traditional file server system. Libraries are, like lists, a fundamental building block in a SharePoint site.

-

- Lessons

- Library Templates

- Creating Libraries

- Creating a Document Library and Adding Columns

- Managing Documents and Versioning

- Checking Out Documents

- Deleting and Restoring Documents

- Versioning

- Lab : Working with Team Site Libraries

- Lab : Creating Libraries

- Lab : Document Versioning

- After completing this module, students will be able to:

-

- Create new libraries using library templates.

- Work with the different libraries in a default Team Site.

- Add columns to a library.

- Check out documents for editing.

- Delete and restore documents from document libraries.

- Enable versioning on a library.

- Revert a library document to an earlier version.

- Module 5: Working with Lists and Library Views

- Views provide a flexible system to display SharePoint list and library data in an easy-to-read and easy-to-use manner. Every SharePoint list and library can have multiple views created and configured, and some list and library templates come with special views preconfigured. Views can be defined for personal use or shared use.

-

- Lessons

- Default Views

- Explore Default Views

- Custom Views

- How to Create a Custom View

- Lab : Creating Team Sites

- Lab : Creating a Blog Site

- After completing this module, students will be able to:

-

- Use default views built into lists and libraries.

- Create personal views.

- Create shared views.

- Configure views.

- Set the default view for a list or library.

- Module 6: Working with Sites

- All SharePoint content is accessed through a site. A SharePoint site is the container for lists and libraries and provides a starting point for basic administration. The content, lists, libraries, and basic look and feel of a site is initially determined by the Site Template used to create the site.

- Lessons

- Site Templates

- Creating Sites

- Creating a Team Site

- Site Navigation

- Managing Site Navigation

- Lab : Creating Team Sites

- Lab : Creating a Blog Site

- After completing this module, students will be able to:

-

- Understand what Site Templates are.

- Understand the different types of Site Templates that come "out of the box" with SharePoint.

- Create a new site using Site Templates.

- Create a Project site.

- Create a Team site.

- Create a Blog site.

- Manage the sites listed in the top link bar.

- Module 7: Page Content

- SharePoint offers a couple of ways to add content to the pages in a site. The latest technique and the one implemented by the Team Site template is through wiki style pages. Another method that has been part of SharePoint since the beginning is the use of Web Parts and Web Part pages. Both techniques are similar in the output that can be created, and both Web Part pages and wiki pages share the ability to add Web Parts to them.

- Lessons

- Wiki Library Pages

- Web Part Pages

- Creating a Web Part Page

- Working with Web Parts

- Lab : Working with Wiki Pages

- After completing this module, students will be able to:

- Understand what wiki pages are.

- Understand what Web Part pages and Web Parts are.

- Add content to the Team Site Home page.

- Change the layout of the Team Site Home page.

- Create a Wiki page.

- Create a Web Part page.

- Add Web Parts.

- Module 8: Site Columns and Content Types

- One method of customizing SharePoint, in a way that can be reused throughout the site or site collection or even the whole farm, is to create Site Columns and Content Types. Site columns are the simplest element; they are essentially the same as list and library columns except that you create them at the site level and then they can be used throughout that site and any child site. Content Types are a combination of Site Columns as well as additional settings and information such as document templates and workflows. Content Types, once created, can then be linked to lists and libraries.

- Lessons

- Site Column Gallery

- Creating Site Columns

- Site Content Type Gallery

- Creating Content Types

- Lab : Creating and Working with Content Types

- Lab : Adding a Content Type to a Library

- After completing this module, students will be able to:

- Understand Content Types.

- Create Site Columns.

- Create Content Types.

- Create a document template for a Content Type.

- Assign a Content Type to a list or library.

- Create new items based on a custom Content Type.

- Module 9: Office Integration

- One of the nice features of SharePoint is its ability to integrate with Microsoft Office applications. Note that this chapter explores integration with Office Online products, a browser-based version of Office that allows you to create and modify office documents. There are limits and they do not perform exactly as their locally installed counterparts.

-

- Lessons

- Outlook Integration

- Lab : Outlook Integration

- After completing this module, students will be able to:

- Create an alert.

- Module 10: Managing SharePoint Site Permissions

- Permissions on a SharePoint site are assigned when a site is created. The default is that permissions assigned to the root of a site collection are inherited by child sites. At any time, permissions inheritance can be turned off at a site, list, library, or even at the item level in a list or library. The permissions themselves can be assigned to either SharePoint groups, individual users, or groups created outside of SharePoint such as Windows groups.

- Lessons

- SharePoint Groups

- Assigning Permissions

- Permissions Inheritance

- Lab : Working with SharePoint Permissions

- After completing this module, students will be able to:

- Understand SharePoint groups.

- Create SharePoint groups.

- Assign permission in SharePoint.

- Manage permission inheritance at the site level.

- Manage permission inheritance at the list or library level.

Microsoft:

Course 20764-C: Administering a SQL Database Infrastructure Description section:

Course overview:

The primary audience for this course is individuals who administer and maintain SQL Server databases. These individuals perform database administration and maintenance as their primary area of responsibility, or work in environments where databases play a key role in their primary job.

The secondary audiences for this course are individuals who develop applications that deliver content from SQL Server databases

Ask About Digital learning if time & budget is an issue.

WHAT YOU'LL LEARN

Authenticate and authorize users

Assign server and database roles

Authorize users to access resources

Protect data with encryption and auditing

Describe recovery models and backup strategies

Backup SQL Server databases

Restore SQL Server databases

Automate database management

Configure security for the SQL Server agent

Manage alerts and notifications

Managing SQL Server using PowerShell

Trace access to SQL Server

Monitor a SQL Server infrastructure

Troubleshoot a SQL Server infrastructure

Import and export data

This course comes with 12 months access to the following benefits:

- Practice Labs
- 24x7 Mentoring
- Indexed Class Recordings
- Unlimited Retakes
- Digital Courseware

PREREQUISITES

In addition to their professional experience, students who attend this training should already have the following technical knowledge:

Basic knowledge of the Microsoft Windows operating system and its core functionality.

Working knowledge of Transact-SQL.

Working knowledge of relational databases.

Some experience with database design.

-

- IT professionals with Windows Server 2016 or Windows Server 2019 experience
- Database Administrators

FOLLOW ON CLASSES: **IMPLEMENTING MICROSOFT AZURE INFRASTRUCTURE SOLUTIONS (20533)**

OUTLINE

Module 1: SQL Server Security

Protection of data within your Microsoft SQL Server databases is essential and requires a working knowledge of the issues and SQL Server security features.

This module describes SQL Server security models, logins, users, partially contained databases, and cross-server authorization.

Lessons

Authenticating Connections to SQL Server

Authorizing Logins to Connect to databases

Authorization Across Servers

Partially Contained Databases

Lab : Authenticating Users

Create Logins

Create Database Users

Correct Application Login Issues

Configure Security for Restored Databases

After completing this module, you will be able to:

SQL Server basic concepts.

SQL Server connection authentication.

User login authorization to databases.

Partially contained databases.

Authorization across servers.

Module 2: Assigning Server and Database Roles

Using roles simplifies the management of user permissions. With roles, you can control authenticated users' access to system resources based on each user's job function—rather than assigning permissions user-by-user, you can grant permissions to a role, then make users members of roles. Microsoft SQL Server includes support for security roles defined at server level and at database level.

Lessons

Working with server roles

Working with Fixed Database Roles

Assigning User-Defined Database Roles

Lab : Assigning server and database roles

Assigning Server Roles

Assigning Fixed Database Roles

Assigning User-Defined Database Roles

Verifying Security

After completing this module, you will be able to:

Describe and use server roles to manage server-level security.

Describe and use fixed database roles.

Use custom database roles and application roles to manage database-level security.

Module 3: Authorizing Users to Access Resources

In the previous modules, you have seen how Microsoft SQL Server security is organized and how sets of permissions can be assigned at the server and database level by using fixed server roles, user-defined server roles, fixed database roles, and application roles. The final step in authorizing users to access SQL Server resources is the authorization of users and roles to access server and database objects.

In this module, you will see how these object permissions are managed. In addition to access permissions on database objects, SQL Server provides the ability to determine which users are allowed to execute code, such as stored procedures and functions. In many cases, these permissions and the permissions on the database objects are best configured at the schema level rather than at the level of the individual object. Schema-based permission grants can simplify your security architecture. You will explore the granting of permissions at the schema level in the final lesson of this module.

Lessons

Authorizing User Access to Objects

Authorizing Users to Execute Code

Configuring Permissions at the Schema Level

Lab : Authorizing users to access resources

Granting, Denying, and Revoking Permissions on Objects

Granting EXECUTE Permissions on Code

Granting Permissions at the Schema Level

After completing this module, you will be able to:

Authorize user access to objects.

Authorize users to execute code.

Configure permissions at the schema level.

Module 4: Protecting Data with Encryption and Auditing

When configuring security for your Microsoft SQL Server systems, you should ensure that you meet any of your organization's compliance requirements for data protection. Organizations often need to adhere to industry-specific compliance policies, which mandate auditing of all data access. To address this requirement, SQL Server provides a range of options for implementing auditing.

Another common compliance requirement is the encryption of data to protect against unauthorized access in the event that access to the database files is compromised. SQL Server supports this requirement by providing transparent data encryption (TDE). To reduce the risk of information leakage by users with administrative access to a database, columns containing sensitive data—such as credit card numbers or national identity numbers—can be encrypted using the Always Encrypted feature.

This module describes the available options for auditing in SQL Server, how to use and manage the SQL Server Audit feature, and how to implement encryption.

Lessons

Options for auditing data access in SQL Server

Implementing SQL Server Audit

Managing SQL Server Audit

Protecting Data with Encryption

Lab : Using Auditing and Encryption

Working with SQL Server Audit

Encrypt a Column as Always Encrypted

Encrypt a Database using TDE

After completing this module, you will be able to:

Describe the options for auditing data access.

Implement SQL Server Audit.

Manage SQL Server Audit.

Describe and implement methods of encrypting data in SQL Server.

Implement encryption

Module 5: Recovery Models and Backup Strategies

One of the most important aspects of a database administrator's role is ensuring that organizational data is reliably backed up so that, if a failure occurs, you can recover the data. Even though the computing industry has known about the need for reliable backup strategies for decades—and discussed this at great length—unfortunate stories regarding data loss are still commonplace. A further problem is that, even when the strategies in place work as they were designed, the outcomes still regularly fail to meet an organization's operational requirements.

In this module, you will consider how to create a strategy that is aligned with organizational needs, based on the available backup models, and the role of the transaction logs in maintaining database consistency.

Lessons

Understanding Backup Strategies

SQL Server Transaction Logs

Planning Backup Strategies

Lab : Understanding SQL Server recovery models

Plan a Backup Strategy

Configure Database Recovery Models

After completing this module, you will be able to:

Describe various backup strategies.

Describe how database transaction logs function.

Plan SQL Server backup strategies.

Module 6: Backing Up SQL Server Databases

In the previous module, you learned how to plan a backup strategy for a SQL Server system. You can now learn how to perform SQL Server backups, including full and differential database backups, transaction log backups, and partial backups.

In this module, you will learn how to apply various backup strategies.

Lessons

Backing Up Databases and Transaction Logs

Managing Database Backups

Advanced Database Options

Lab : Backing Up Databases

Backing Up Databases

Performing Database, Differential, and Transaction Log Backups

Performing a Partial Backup

After completing this module, you will be able to:

Perform backups of SQL Server databases and transaction logs.

Manage database backups.

Describe advanced backup options.

Module 7: Restoring SQL Server 2016 Databases

In the previous module, you learned how to create backups of Microsoft SQL Server 2016 databases. A backup strategy might involve many different types of backup, so it is essential that you can effectively restore them.

You will often be restoring a database in an urgent situation. You must, however, ensure that you have a clear plan of how to proceed and successfully recover the database to the required state. A good plan and understanding of the restore process can help avoid making the situation worse.

Some database restores are related to system failure. In these cases, you will want to return the system as close as possible to the state it was in before the failure. Some failures, though, are related to human error and you might wish to recover the system to a point before that error. The point-in-time recovery features of SQL Server 2016 can help you to achieve this.

Because they are typically much larger, user databases are more likely to be affected by system failures than system databases. However, system databases can be affected by failures, and special care should be taken when recovering them. In particular, you need to understand how to recover each system database because you cannot use the same process for all system databases.

In this module, you will see how to restore user and system databases and how to implement point-in-time recovery.

Lessons

Understanding the Restore Process

Restoring Databases

Advanced Restore Scenarios

Point-in-Time Recovery

Lab : Restoring SQL Server Databases

Restoring a Database Backup

Restring Database, Differential, and Transaction Log Backups

Performing a Piecemeal Restore

After completing this module, you will be able to:

Explain the restore process.

Restore databases.

Perform advanced restore operations.

Perform a point-in-time recovery.

Module 8: Automating SQL Server Management

The tools provided by Microsoft SQL Server make administration easy when compared to some other database engines. However, even when tasks are easy to perform, it is common to have to repeat a task many times. Efficient database administrators learn to automate repetitive tasks. This can help to avoid situations where an administrator forgets to execute a task at the required time. Perhaps more importantly, the automation of tasks helps to ensure that they are performed consistently, each time they are executed.

This module describes how to use SQL Server Agent to automate jobs, how to configure security contexts for jobs, and how to implement multiserver jobs.

Lessons

Automating SQL Server management

Working with SQL Server Agent

Managing SQL Server Agent Jobs

Multi-server Management

Lab : Automating SQL Server Management

Create a SQL Server Agent Job

Test a Job

Schedule a Job

Configure Master and Target Servers

After completing this module, you will be able to:

Describe methods for automating SQL Server Management.

Configure jobs, job step types, and schedules.

Manage SQL Server Agent jobs.

Configure master and target servers.

Module 9: Configuring Security for SQL Server Agent

Other modules in this course have demonstrated the need to minimize the permissions that are granted to users, following the principle of "least privilege." This means that users have only the permissions that they need to perform their tasks. The same logic applies to the granting of permissions to SQL Server Agent. Although it is easy to execute all jobs in the context of the SQL Server Agent service account, and to configure that account as an administrative account, a poor security environment would result from doing this. It is important to understand how to create a minimal privilege security environment for jobs that run in SQL Server Agent.

Lessons

Understanding SQL Server Agent Security

Configuring Credentials

Configuring Proxy Accounts

Lab : Configuring Security for SQL Server Agent

Analyzing Problems in SQL Server Agent

Configuring a Credential

Configuring a Proxy Account

Configuring and testing the Security Context of a Job

After completing this module, you will be able to:

Explain SQL Server Agent security.

Configure credentials.

Configure proxy accounts.

Module 10: Monitoring SQL Server with Alerts and Notifications

One key aspect of managing Microsoft SQL Server in a proactive manner is to make sure you are aware of problems and events that occur in the server, as they happen. SQL Server logs a wealth of information about issues. You can configure it to advise you automatically when these issues occur, by using alerts and notifications. The most common way that SQL Server database administrators receive details of events of interest is by email message. This module covers the configuration of Database Mail, alerts, and notifications for a SQL Server instance, and the configuration of alerts for Microsoft Azure SQL Database.

Lessons

Monitoring SQL Server Errors

Configuring Database Mail

Operators, Alerts, and Notifications

Alerts in Azure SQL Database

Lab : Monitoring SQL Server with Alerts and Notifications

Configuring Database Mail

Configuring Operators

Configuring Alerts and Notifications

Testing Alerts and Notifications

After completing this module, you will be able to:

Monitor SQL Server errors.

Configure database mail.

Configure operators, alerts, and notifications.

Work with alerts in Azure SQL Database.

Module 11: Introduction to Managing SQL Server by using PowerShell

This module looks at how to use Windows PowerShell with Microsoft SQL Server. Businesses are constantly having to increase the efficiency and reliability of maintaining their IT infrastructure; with PowerShell, you can improve this efficiency and reliability by creating scripts to carry out tasks. PowerShell scripts can be tested and applied multiple times to multiple servers, saving your organization both time and money.

Lessons

Getting Started with Windows PowerShell

Configure SQL Server using PowerShell

Administer and Maintain SQL Server with PowerShell

Managing Azure SQL Databases using PowerShell

Lab : Using PowerShell to Manage SQL Server

Getting Started with PowerShell

Using PowerShell to Change SQL Server settings

After completing this module, you will be able to:

Describe the benefits of PowerShell and its fundamental concepts.

Configure SQL Server by using PowerShell.

Administer and maintain SQL Server by using PowerShell.

Manage an Azure SQL Database by using PowerShell.

Module 12: Tracing Access to SQL Server with Extended events

Monitoring performance metrics provides a great way to assess the overall performance of a database solution. However, there are occasions when you need to perform more detailed analysis of the activity occurring within a Microsoft SQL Server instance—to troubleshoot problems and identify ways to optimize workload performance.

SQL Server Extended Events is a flexible, lightweight event-handling system built into the Microsoft SQL Server Database Engine. This module focuses on the architectural concepts, troubleshooting strategies and usage scenarios of Extended Events.

Lessons

Extended Events Core Concepts

Working with Extended Events

Lab : Extended Events

Using the System_Health Extended Events Session

Tracking Page Splits Using Extended Events

After completing this module, you will be able to:

Describe Extended Events core concepts.

Create and query Extended Events sessions.

Module 13: Monitoring SQL Server

The Microsoft SQL Server Database Engine can run for long periods without the need for administrative attention. However, if you regularly monitor the activity that occurs on the database server, you can deal with potential issues before they arise. SQL Server provides a number of tools that you can use to monitor current activity and record details of previous activity. You need to become familiar with what each of the tools does and how to use them. It is easy to become overwhelmed by the volume of output that monitoring tools can provide, so you also need to learn techniques for analyzing their output.

Lessons

Monitoring activity

Capturing and Managing Performance Data

Analyzing Collected Performance Data

SQL Server Utility

Lab : Monitoring SQL Server

After completing this module, you will be able to:

Monitor current activity.

Capture and manage performance data.

Analyze collected performance data.

Configure SQL Server Utility.

Module 14: Troubleshooting SQL Server

Database administrators working with Microsoft SQL Server need to adopt the important role of troubleshooter when issues arise—particularly if users of business-critical applications that rely on SQL Server databases are being prevented from working. It is important to have a solid methodology for resolving issues in general, and to be familiar with the most common issues that can arise when working with SQL Server systems.

Lessons

A Trouble Shooting Methodology for SQL Server

Resolving Service Related Issues

Resolving Connectivity and Log-in issues

Lab : Troubleshooting Common Issues

Troubleshoot and Resolve a SQL Login Issue

Troubleshoot and Resolve a Service Issue

Troubleshoot and Resolve a Windows Login Issue

Troubleshoot and Resolve a Job Execution Issue

Troubleshoot and Resolve a Performance Issue

After completing this module, you will be able to:

Describe a troubleshooting methodology for SQL Server.

Resolve service-related issues.

Resolve login and connectivity issues.

Module 15: Importing and Exporting Data

While a great deal of data residing in a Microsoft SQL Server system is entered directly by users who are running application programs, there is often a need to move data in other locations, to and from SQL Server.

SQL Server provides a set of tools you can use to transfer data in and out. Some of these tools, such as the bcp (Bulk Copy Program) utility and SQL Server Integration Services, are external to

the database engine. Other tools, such as the BULK INSERT statement and the OPENROWSET function, are implemented in the database engine. With SQL Server, you can also create data-tier applications that package all the tables, views, and instance objects associated with a user database into a single unit of deployment.

In this module, you will explore these tools and techniques so that you can import and export data to and from SQL Server.

Lessons

Transferring Data to and from SQL Server

Importing and Exporting Table Data

Using bcp and BULK INSERT to Import Data

Deploying and Upgrading Data-Tier Application

Lab : Importing and Exporting Data

Import and Excel Data Using the Import Wizard

Import a Delimited Text File Using bcp

Import a Delimited Text File using BULK INSERT

Create and Test an SSIS Package to Extract Data

Deploy a Data-Tier Application

After completing this module, you will be able to:

Describe tools and techniques for transferring data.

Import and export table data.

Use bcp and BULK INSERT to import data.

Use data-tier applications to import and export database applications.

Microsoft

ADMINISTERING SYSTEM CENTER CONFIGURATION MANAGER AND INTUNE (20696)

Description section:

Course overview:

In this course 5-day class, you will practice configuring and managing clients and devices using Microsoft System Center Configuration Manager, Microsoft Intune, and its associated site systems. You will learn day-to-day management tasks including how to manage software, client health, hardware and software inventory, applications, and integration with Microsoft Intune. You also will discover how to optimize System Center 2012 Endpoint Protection, manage compliance, and create management queries and reports.

This course incorporates materials from the Official Microsoft Learning Product 20696: Administering System Center Configuration Manager and Intune and it can assist you in your preparation for Exam 70-696: Administering System Center Configuration Manager and Intune.

Ask About Digital learning if time & budget is an issue.

WHAT YOU'LL LEARN

- Manage desktops and devices in the enterprise

- Prepare the infrastructure to support desktop and device management

- Deploy and manage Configuration Manager clients

- Configure, manage, and monitor hardware and software inventory, and use Asset Intelligence and software metering

- Distribute and manage content used for deployments

- Deploy and manage applications

- Manage mobile devices by integrating Microsoft Intune with Configuration Manager

- Maintain software updates for managed PCs

- Implement Endpoint Protection for managed PCs

- Maintain Configuration Manager sites and site systems

This course comes with 12 months access to the following benefits:

- Practice Labs

- 24x7 Mentoring

- Indexed Class Recordings

- Unlimited Retakes

- Digital Courseware

PREREQUISITES

You must have system administrator-level working knowledge of:

- Networking fundamentals, including common networking protocols, topologies, hardware, media, routing, switching and addressing

- Active Directory Domain Services (AD DS) principles and fundamentals of AD DS management

- Basic understanding of scripting and Windows PowerShell syntax

- Basic understanding of Windows Server roles and services

- Basic understanding of management tasks using System Center 2012 R2 Configuration Manage

  Implementing and Managing Windows 10 (20697-1)

  Deploying and Managing Windows 10 using Enterprise Services (20697-2)

  Administering Windows Server 2012 (20411)

IT professionals who deploy, manage, and maintain PCs, devices, and applications across medium, large, and enterprise organizations and who use System Center 2012 R2 Configuration Manager and Microsoft Intune together, to manage and deploy PCs, devices, and applications

Follow Up Courses: Check with your Rep for advise on next steps.

Certifications: MCSE Mobility

OUTLINE

VIRTUAL CLASSROOM LIVE OUTLINE
1. Managing Computer and Mobile Devices in the Enterprise

- Overview of systems management by using enterprise-management solutions
- Overview of Configuration Manager and Cloud Services Architecture
- Overview of the Configuration Manager Administrative Tools
- Monitoring and Troubleshooting a Configuration Manager Site
- Introduction to Queries and Reports

   2. Preparing the Management Infrastructure to Support PCs and Mobile Devices

- Configuring Site Boundaries and Boundary Groups
- Configuring Resource Discovery
- Configuring the Exchange Server Connector for Mobile Device Management
- Configuring User and Device Collections

   3. Deploying and Managing Clients

- Overview of the Configuration Manager Client
- Deploying the Configuration Manager Client
- Managing Client Settings in Configuration Manager

   4. Managing Inventory for PCs and Applications

- Overview of the Inventory Collection

- Configuring Hardware and Software Inventory

- Managing Inventory Collection

- Configuring Software Metering

- Configuring Asset Intelligence

    5. Distributing and Managing Content Used for Deployments

- Preparing the Infrastructure for Content Management

- Distributing and Managing Content on Distribution Points

    6. Deploying and Managing Applications

- Overview of Application Management

- Creating Applications

- Deploying Applications

- Managing Applications

- Deploying and Managing Windows Store Apps

    7. Maintaining Software Updates for Managed PCs

- Overview of Software Updates

- Preparing a Configuration Manager Site for Software Updates

- Managing Software Updates

- Configuring Automatic Deployment Rules

- Monitoring and Troubleshooting Software Updates

    8. Implementing Endpoint Protection for Managed PCs

- Overview of Endpoint Protection in Configuration Manager

- Configuring and Monitoring Endpoint Protection Policies

    9. Managing Compliance and Secure Data Access

- Overview of Compliance Settings

- Configuring Compliance Settings

- Viewing Compliance Results

    10. Managing Operating System Deployments

- An overview of operating-system deployment

- Preparing a site for operating-system deployment

- Deploying an operating-system

11. Mobile Device Management Using Configuration Manager and Microsoft Intune

- Overview of mobile-device management

- Managing mobile devices with on-premises infrastructure

- Managing mobile devices by using Configuration Manager and Intune

- Managing settings and protecting data on mobile devices

- Deploying applications to mobile devices

12. Managing and Maintaining a Configuration Manager Site

- Configuring role-based administration

- Configuring remote tools

- Overview of Configuration Manager site maintenance

- Performing backup and recovery of a Configuration Manager site

LABS

VIRTUAL CLASSROOM LIVE LABS
Lab 1: Exploring the Configuration Manager Tools

- Searching in the Configuration Manager Console

- Using Windows PowerShell with Configuration Manager

- Managing Components by Using Configuration Manager Service Manager

- Monitoring Site and Component Status

- Reviewing Log Files by Using Configuration Manager Trace Log Tool

Lab 2: Creating Queries and Configuring Reporting Services

- Creating Data Queries

- Creating Subselect Queries

- Configuring a Reporting Services Point

Lab 3: Configuring Boundaries and Resource Discovery

- Configuring Active Directory Discovery Methods

Lab 4: Configuring User and Service Collections

- Creating a Device Collection

- Creating a User Collection

- Configuring a Maintenance Window

Lab 5: Deploying the Microsoft System Center Configuration Manager Client Software

- Preparing the Site for Client Installation

- Deploying the Configuration Manager client software by using client push installation

Lab 6: Configuring and Monitoring Client Status

- Configuring and Monitoring Client Health Status

Lab 7: Manage Client Settings

Lab 8: Configuring and Managing Inventory Collection

Lab 9: Configuring Software Metering

Lab 10: Configuring and Managing Asset Intelligence

- Preparing the Site for Asset Intelligence

- Configuring Asset Intelligence

- Customizing the Asset Intelligence Catalog

- Viewing the Asset Intelligence Reports

Lab 11: Distributing and Managing Content for Deployments

- Installing a New Distribution Point

- Managing Content Distribution

Lab 12: Creating and Deploying Applications

- Installing and Configuring the Application Catalog Roles

- Creating Applications with Requirements

- Deploying Applications

Lab 13: Managing Application Supersedence and Removal

- Managing Application Supersedence

- Uninstalling the Excel Viewer Application

Lab 14: Using Configuration Manager to Deploy Windows Store Apps

- Configuring Support for Sideloading Windows Store Apps

- Configuring a Windows Store App

- Deploying Windows 10 Apps to Users

Lab 15: Configuring the Site for Software Updates

- Configuring and Synchronizing the Software Update Point

Lab 16: Deploying and Managing Software Updates

- Determining Software Update Compliance
- Deploying Software Updates to Clients

Lab 17: Implementing Microsoft System Center Endpoint Protection

- Configuring the Endpoint Protection Point and Client Settings
- Configuring and Deploying Endpoint Protection Policies
- Monitoring Endpoint Protection

Lab 18: Managing Compliance Settings

- Managing Configuration Items and Baselines
- Viewing Compliance Settings and Reports
- Configuring Remediation in Compliance Settings
- Using Compliance Information to Create Collections
- Configuring Automatic Deployment Rules

Lab 19: Preparing a Site for Operating-System Deployment

- Managing the Site System Roles Used to Support Operating-System Deployment
- Managing Packages to Support Operating-System Deployment

Lab 20: Deploying Operating-System Images for Bare-Metal Installations

- Preparing the Operating-System Image
- Creating a Task Sequence to Deploy an Image
- Deploying an Image

Lab 21: Managing Mobile Devices with On-Premises Infrastructure

- Preparing Configuration Manager Prerequisites for On-Premises Mobile-Device Management
- Enrolling and Configuring a Windows Phone 10 Mobile Device

Lab 22: Configuring Role-Based Administration

- Configuring a New Administrative User

Lab 23: Configuring Remote Tools

- Configuring the Remote Tools Client Settings and Permissions
- Managing Desktops by Using Remote Control

Lab 24: Maintaining a Configuration Manager Site

- Configuring Maintenance Tasks in Configuration Manager

- Configuring the Backup Site Server Task

- Recovering a Site from a Backup

UPGRADING YOUR SKILLS TO WINDOWS SERVER 2016/2019 MCSA

   New – Upgrade your skills from Windows Server 2008 or Windows Server 2012 to Windows Server 2016.

Description section:

Course overview:

In this course 5-day course, you will learn how to implement and configure new features and functionality in Windows Server 2016. This course is designed for IT professionals who want to upgrade their technical skills from Windows Server 2008 or Windows Server 2012 to Windows Server 2016.

This is not a product-upgrade course, detailing considerations for migrating and upgrading students' specific environment to Windows Server 2016. Rather, this course presumes a high level of knowledge about previous Windows Server technologies and skills, as they pertain to Windows Server 2016

This course incorporates material from the Official Microsoft Learning Product 20743: Upgrading Your Skills to Windows Server 2016 MCSA and can assist you in preparing for the 70-743: Upgrading Your Skills to MCSA: Windows Server 2016 exam.

Ask About Digital learning if time & budget is an issue.

WHAT YOU'LL LEARN

- Install and configure Windows Server 2016
- Storage in Windows Server 2016
- Implement directory services
- Implement Active Directory Federation Services (AD FS)
- Networking
- Implement Hyper-V
- Configure advanced networking features
- Implement software-defined networking
- Implement remote access
- Deploy and manage Windows and Hyper-V containers
- Implement failover clustering
- Implement failover clustering by using virtual machines
- Monitor and review Office 365 services, and troubleshoot Office 365 issues
- Plan and implement identity federation between on-premises AD DS and Azure AD

This course comes with 12 months access to the following benefits:

- Practice Labs
- 24x7 Mentoring
- Indexed Class Recordings
- Unlimited Retakes
- Digital Courseware

PREREQUISITES

- At least two years of experience in deploying and managing Windows Server 2012 or Windows 2008 environments
- Experience with day-to-day Windows Server 2012 or Windows Server 2008 system administration management and maintenance tasks
- Experience with Windows networking technologies and implementation

- Experience with Active Directory technologies and implementation

- Experience with Windows Server virtualization technologies and implementation

- Knowledge equivalent to the MCSA credentials of Windows Server 2008 or Windows Server 2012 (or equivalent knowledge)

Installation, Storage, and Compute with Windows Server 2016 (20740)

NETWORKING WITH WINDOWS SERVER 2016 (20741)

I   DENTITY WITH WINDOWS SERVER 2016 (20742)

-

WHO SHOULD ATTEND

- IT professionals with Windows Server 2008 or Windows Server 2012 experience

- Server administrators carrying out day-to-day management and administrative tasks and want to update their skills and knowledge to Windows Server 2016

Related Certifications:

MCSA Windows Server 2016

FOLLOW ON CLASSES: **IMPLEMENTING MICROSOFT AZURE INFRASTRUCTURE SOLUTIONS (20533)**

OUTLINE

. Installing and Configuring Windows Server 2016

- Introducing Windows Server 2016

- Preparing for upgrades and migrations

- Migrating server roles and workloads

- Windows Server activation models

2. Overview of Storage in Windows Server 2016

- Configuring Internet SCSI (iSCSI) storage

- Configuring the Storage Spaces feature in Windows Server 2016
- Implementing the Data Deduplication feature

3. Implementing the Directory Services Feature

- Deploying AD DS domain controllers
- Implementing service accounts
- What is Azure AD?

4. Implementing AD FS

- Overview of AD FS
- Deploying AD FS
- Implementing AD FS for a single organization
- Implementing Web Application Proxy
- Implementing Azure AD FS SSO with Microsoft Online Services

5. Implementing Network Services

- Overview of networking enhancements
- Implementing the IP address management
- Managing IP address spaces with IPAM

6. Implementing Hyper-V

- Configuring the Hyper-V role in Windows Server 2016
- Configuring Hyper-V storage
- Configuring Hyper-V networking
- Configuring Hyper-V virtual machines

7. Configuring Advanced Networking Features

- Overview of high-performance networking features
- Configuring advanced Hyper-V networking features

8. Implementing software defined networking

- Overview of software-defined networking
- Implementing network virtualization
- Implementing the Network Controller feature

9. Implementing Remote Access

- Remote access overview
Implementing DirectAccess
Implementing a virtual private network (VPN)

   10. Deploying and Managing Windows Server and Hyper-V Containers

- Overview of Windows Server 2016 containers

- Deploying Windows Server and Hyper-V containers

- Installing, configuring, and managing containers

   11. Implementing Failover Clustering

- Overview of failover clustering

- Configuring highly-available applications and services on a failover cluster

- Maintaining a failover cluster

- Implementing a stretch cluster

   12. Implementing Failover Clustering with Windows Server 2016 Hyper-V

- Overview of the integration of Hyper-V Server 2016 with failover clustering

- Implementing Hyper-V virtual machines on failover clusters

- Implementing Windows Server 2016 Hyper-V virtual machine migration

- Implementing the Hyper-V Replica feature

 LABS

VIRTUAL CLASSROOM LIVE LABS
Lab 1: Installing and Configuring Nano Server

- Installing Nano Server

- Completing post-installation tasks on Nano Server

   Lab 2: Implementing and Managing Storage

- Implementing File Server Resource Manager (FSRM)

- Configuring iSCSI storage

   Lab 3: Implementing and Managing Advanced Storage Solutions

- Configuring redundant storage spaces

- Implementing the Storage Spaces Direct feature

   Lab 4: Implementing and Managing AD DS

- Cloning an domain controller
- Implementing service accounts

Lab 5: Implementing AD FS

- Installing and configuring AD FS
- Configuring an internal application for AD FS

Lab 6: Implementing Network Services

- Configuring DNS policies
- Configuring DHCP failover
- Configuring IPAM

Lab 7 : Implementing Server Virtualization with Hyper-V

- Installing the Hyper-V server role
- Configuring virtual networking
- Creating and configuring a VM

Lab 8: Configuring Advanced Hyper-V Networking Features

- Creating and using Microsoft Hyper-V virtual switches
- Configuring and using the advanced features of a virtual switch

Lab 9: Deploying Network Controller

Lab 10: Implementing DirectAccess

- Configuring DirectAccess by using the Getting Started Wizard
- Testing DirectAccess

Lab 11: Installing and Configuring Containers

- Installing Docker

Lab 12: Implementing Failover Clustering

- Configuring iSCSI storage
- Configuring a failover cluster
- Deploying and configuring a highly-available file server
- Validating the deployment of a highly-available file server
- Configuring the Cluster-Aware Updating feature on the failover cluster

Lab 13: Implementing Failover Clustering with Windows Server 2016 Hyper-V

- Configuring Hyper-V Replica

- Configuring a failover cluster for Hyper-V

- Configuring a highly available virtual machine

EC Council

Certified Ethical Hacker (CEH)

Course Overview

The Certified Ethical Hacker (CEH) program is the core of the most desired information security training system any information security professional will ever want to be in. The CEH, is the first part of a 3-part EC-Council Information Security Track which helps you master hacking technologies. You will become a hacker, but an ethical one.

What You will learn:

CEH v9 (Certified Ethical Hacker) training and certification boot camp will immerse the students into a hands-on environment where they will be shown how to conduct ethical hacking. They will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! They will 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 lead into scanning and attacking their own networks. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. All of this will be done without harming any real network. 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 class they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council Certified Ethical Hacker v9 exam 312-50

This course includes:

- All Courseware
- Practice exams via Portal
- Optional Evening Review Sessions in addition to the 5 days of training
- Pre/Post Assessments
- Certification Exam

PREREQUISITES

- Strong knowledge of TCP/IP
- Information systems and security background
- Minimum of 12 months of experience in networking technologies

WHO SHOULD ATTEND

- Security Officers
- Auditors
- Network Administrators
- Firewall Administrators
- Security Professionals
- Anyone who is concerned about the integrity of the network infrastructure

FOLLOW UP COURSES:

ECSA AND OTHER EC COUNCIL CLASSES

CERTIFICATION:

- 312-50 – Certified Ethical Hacker (ANSI)
- Exam Code: 312-50 (ECC EXAM), 312-50 (VUE)
- 312-99 – Certified Network Defense Architect (CNDA)

OUTLINE & LABS

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. System Hacking
6. Malware Threats
7. Sniffing
8. Social Engineering
9. Denial of Service
10. Session Hijacking
11. Hacking Web Servers
12. Hacking Web Applications
13. SQL Injection
14. Hacking Wireless Networks
15. Hacking Mobile Platforms
16. Evading IDS, Firewalls, and Honeypots
17. Cloud Computing
18. Cryptography

EC Council Certified Security Analyst (ECSA)

Course Overview

The ECSA penetration testing course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report

What You will learn:

As the ECSA course is a fully hands-on program, the exercises cover real world scenario. By practicing the skills that are provided to you in the ECSA class, we are able to bring you up to speed with the latest threats that organizations may be vulnerable to. This can be achieved with the EC-Council Cyber Range iLabs. It allows you to dynamically access a host of Virtual Machines precongured with vulnerabilities, exploits, tools, and scripts from anywhere with an internet connection. Our web portal enables you to launch an entire range of target machines and access them remotely with one simple click. It is the most cost e-ective and easy to use live range lab solution available. With iLabs, lab exercises can be accessed 24x7, allowing the student to practice skills in a safe and fully functional network anytime it is convenient. Our guided step-by-step labs include exercises with detailed tasks, supporting tools, and additional materials as well as our state-of-the-art "Open Environment" allowing you to launch a complete live range open for any form of hacking or testing. Available target machines are completely

virtualized, allowing you to control and reset machines quickly and easily with no required instructor or administrative interaction.

This course includes:

- All Courseware
- Practice exams via Portal
- Optional Evening Review Sessions in addition to the 5 days of training
- Pre/Post Assessments
- Certification Exam

PREREQUISITES

- CEH or core Ethical Hacking Skills

WHO SHOULD ATTEND

- Ethical Hackers
- Penetration Testers
- Network server administrators
- Firewall Administrators
- Security Testers

- System Administrators and Risk Assessment professionals

CERTIFICATION:

- ECSA

The ECSA exam has 2 required testing stages. The report writing stage requires candidates to perform various penetration testing exercises on EC-Council's iLabs before submitting a penetration test report to EC-Council for assessment. From the commencement of the 5 day class and the activation of the ECSA Dashboard on ASPEN, you will have 60 days in total to submit your penetration testing report. Candidates who submit reports to the required standards will be permitted to take the multiple choice exam. The multiple choice exam is proctored online through the EC-Council Exam portal.

OUTLINE & LABS

19. Security Analysis and Penetration Testing Methodologies

20. TCP IP Packet Analysis

21. Pre-penetration Testing Steps

22. Information Gathering Methodology

23. Vulnerability Analysis

24. External Network Penetration Testing Methodology

25. Internal Network Penetration Testing Methodology

26. Firewall Penetration Testing Methodology

27. IDS Penetration Testing Methodology

28. Web Application Penetration Testing Methodology

29. SQL Penetration Testing Methodology

30. Database Penetration Testing Methodology

31. Wireless Network Penetration Testing Methodology

32. Mobile Devices Penetration Testing Methodology

33. Cloud Penetration Testing Methodology

34. Report Writing and Post Test Actions

CERTIFIED NETWORK DEFENDER PROGRAM (CND)

Course Overview

Organizational focus on cyber defense is more important than ever as cyber breaches have a far greater financial impact and can cause broad reputational damage.

Despite best efforts to prevent breaches, many organizations are still being compromised. Therefore organizations must have, as part of their defense mechanisms, trained network engineers who are focused on protecting, detecting, and responding to the threats on their networks.

Network administrators spends a lot of time with **network environments**, and are familiar with network components, traffic, performance and utilization, network topology, location of each system, security policy, etc.

So, organizations can be much better in defending themselves from vicious attacks if the IT and network administrators equipped with adequate network security skills .Thus Network administrator can play a significant role in network defense and become first line of defense for any organizations.

There is no proper tactical network security training that is made available for network administrators which provides them core network security skills.

What You will learn:

Students enrolled in the Certified Network Defender course, will gain a detailed understanding and hands on ability to function in real life situations involving network defense. They will gain the technical depth required to actively design a secure network in your organization. This program will be akin to learning math instead of just using a calculator. This course gives you the fundamental understanding of the true construct of data transfer, network technologies, software technologies so that you understand how networks operate, understand what software is automating and how to analyze the subject material.

You will learn how to protect, detect and respond to the network attacks. You will learn network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN and firewall configuration. You will then learn the intricacies of network traffic signature, analysis and vulnerability scanning which will help you when you design greater network security policies and successful incident response plans. These skills will help you foster resiliency and continuity of operations during attacks.
.

This course includes:

- All Courseware
- Practice exams via Portal
- Optional Evening Review Sessions in addition to the 5 days of training
- Pre/Post Assessments
- Certification Exam

PREREQUISITES

YOU SHOULD BE WELL-VERSED IN CYBER SECURITY FUNDAMENTALS.

WHO SHOULD ATTEND

- Network Administrators
- Network security Administrators
- Network Security Engineer
- Network Defense Technicians
- CND Analyst
- Security Analyst
- Security Operator
- Anyone who involves in network operations

FOLLOW UP COURSES:

CHECK WITH YOUR REPRESENTATIVE FOR THE BEST OPTIONS FOR YOU

CERTIFICATION:

CND

- **Exam title:** CND
- **Number of questions:** 100
- **Duration:** 4 Hours
- **Availability:** ECC Exam
- **Test Format:** Interactive Multiple Choice Questions

OUTLINE & LABS

Module 01: Computer Network and Defense Fundamentals.

Module 02: Network Security Threats, Vulnerabilities, and Attacks.

Module 03: Network Security Controls, Protocols, and Devices.

Module 04: Network Security Policy Design and Implementation.

Module 05: Physical Security.

Module 06: Host Security.

Module 07: Secure Firewall Configuration and Management.

Module 08: Secure IDS Configuration and Management.

Module 09: Secure VPN Configuration and Management.

Module 10: Wireless Network Defense.

Module 11: Network Traffic Monitoring and Analysis.

Module 12: Network Risk and Vulnerability Management.

Module 13: Data Backup and Recovery.

Module 14: Network Incident Response and Management.

EC Council Computer Hacking Forensics Investigator (C|HFI)

Course Overview

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification will fortify the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.

What You will learn:

- Perform incident response and forensics

- Perform electronic evidence collections

- Perform digital forensic acquisitions

- Perform bit-stream Imaging/acquiring of the digital media seized during the process of investigation.

- Examine and analyze text, graphics, multimedia, and digital images

- Conduct thorough examinations of computer hard disk drives, and other electronic data storage media

- Recover information and electronic data from computer hard drives and other data storage devices

- Follow strict data and evidence handling procedures

- Maintain audit trail (i.e., chain of custody) and evidence integrity

- Work on technical examination, analysis and reporting of computer-based evidence

- Prepare and maintain case files

- Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images and other files

- Gather volatile and non-volatile information from Windows, MAC and Linux

- Recover deleted files and partitions in Windows, Mac OS X, and Linux

- Perform keyword searches including using target words or phrases

- Investigate events for evidence of insider threats or attacks

- Support the generation of incident reports and other collateral

- Investigate and analyze all response activities related to cyber incidents

- Plan, coordinate and direct recovery activities and incident analysis tasks

- Examine all available information and supporting evidence or artefacts related to an incident or event

- Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents

- Conduct reverse engineering for known and suspected malware files

- Perform detailed evaluation of the data and any evidence of activity in order to analyze the full circumstances and implications of the event

- Identify data, images and/or activity which may be the target of an internal investigation

- Establish threat intelligence and key learning points to support pro-active profiling and scenario modelling

- Search file slack space where PC type technologies are employed

- File MAC times (Modified, Accessed, and Create dates and times) as evidence of access and event sequences

- Examine file type and file header information

- Review e-mail communications including web mail and Internet Instant Messaging programs

- Examine the Internet browsing history

- Generate reports which detail the approach, and an audit trail which documents actions taken to support the integrity of the internal investigation process

- Recover active, system and hidden files with date/time stamp information

- Crack (or attempt to crack) password protected files

- Perform anti-forensics detection

- Maintain awareness and follow laboratory evidence handling, evidence examination, laboratory safety, and laboratory security policy and procedures

- Play a role of first responder by securing and evaluating a cybercrime scene, conducting preliminary interviews, documenting crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, reporting of the crime scene

- Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred

- Apply advanced forensic tools and techniques for attack reconstruction

- Perform fundamental forensic activities and form a base for advanced forensics

- Identify and check the possible source/incident origin

- Perform event co-relation

- Extract and analyze logs from various devices such as proxies, firewalls, IPSes, IDSes, Desktops, laptops, servers, SIM tools, routers, switches, AD servers, DHCP servers, Access Control Systems, etc.

- Ensure that reported incident or suspected weaknesses, malfunctions and deviations are handled with confidentiality

- Assist in the preparation of search and seizure warrants, court orders, and subpoenas

- Provide expert witness testimony in support of forensic examinations conducted by the examiner

This course includes:

- All Courseware
- Practice exams via Portal
- Optional Evening Review Sessions in addition to the 5 days of training
- Pre/Post Assessments
- Certification Exam

PREREQUISITES

• IT/FORENSICS PROFESSIONALS WITH BASIC KNOWLEDGE ON IT/CYBER SECURITY, COMPUTER FORENSICS, AND INCIDENT RESPONSE • PRIOR COMPLETION OF CEH TRAINING WOULD BE AN ADVANTAGE.

WHO SHOULD ATTEND

THE CHFI PROGRAM IS DESIGNED FOR ALL IT PROFESSIONALS INVOLVED WITH INFORMATION SYSTEM SECURITY, COMPUTER FORENSICS, AND INCIDENT RESPONSE.

- Police and other law enforcement personnel
- Defense and Military personnel
- e-Business Security professionals
- Systems administrators
- Legal professionals
- Banking, Insurance and other professionals
- Government agencies
- IT managers

FOLLOW UP COURSES:

CHECK WITH YOUR REPRESENTATIVE FOR THE BEST OPTIONS FOR YOU

CERTIFICATION:

- Other EC Council classes available. Consult with your representative.

OUTLINE & LABS

Module 1. Computer forensics in today's world

Module 2. Computer forensics investigation process

Module 3. Understanding hard disks and file systems

Module 4 Data acquisition and duplication

Module 5. Defeating anti-forensics techniques

Module 6. Operating system forensics

Module 7. Network forensicsCloud Penetration Testing Methodology

8. Investigating web attacks

Module 9. Database forensic

Module 10. Cloud forensic

Module 11. Malware forensic

Module 12. Investigating email crimes

Module 13. Mobile forensic

Module 14. Forensics report writing and presentation

(CISA)

ISACA

CERTIFIED INFORMATION SYSTEM AUDITOR

Course overview

Join fellow CISA exam candidates along with a CISA-certified trainer for a unique exam prep experience. The CISA Exam Prep Course is an intensive, cram-style course that will cover some of the more challenging topics from the CISA job practice. Drill through sample exam items, ask your most pressing questions and get the answers to build your confidence as you prepare for exam day

WHAT YOU'LL LEARN

• Auditing Process Overview

• IT Governance

• Lifecycle Management

- System Infrastructure Control

- IS Hardware and Architecture

- Information Security for IT Delivery and Support

- Protecting Logical Assets

- Physical Security

- Business Continuity and Disaster Recovery

WHATS INCLUDED:

- All Courseware
- Practice exams
- Exam Guidance

PREREQUISITES

- At least five years of work experience with IT systems, auditing and information security
- Familiarity with TCP/IP
- Familiarity with Windows, Linux and UNIX operating systems
- Helpful to have a CompTIA Security+ certification

WHO SHOULD ATTEND

- CISA Exam Candidates
- Audit professionals with 3-5 years of experience including:
- Auditors

- Managers
- Information Security Officers
- Security Engineers
- IT Security Professionals

FOLLOW UP COURSES:

CISM

Certifications:

CISA

OUTLINE & LABS

Module 1: Audit Process

- Lesson 1A: Risk and Audit
- Lesson 1B: Guidelines and Standards

Module 2: IT Governance

- Lesson 2A: Best Practices for IT Governance
- Lesson 2B: Management Practices
- Lesson 2C: Responsibilities and Roles

Module 3: Lifecycle Management

- Lesson 3A: Project Management
- Lesson 3B: Business Application Development
- Lesson 3C: IS Maintenance Practices

Module 4: System Infrastructure Control

- Lesson 4A: Controls for Auditing Applications
- Lesson 4B: Application System Development and Business Application Systems

Module 5: IS Hardware and Architecture

- Lesson 5A: IS Operations and Hardware

- Lesson 5B: SDLC
- Lesson 5C: Databases

Module 6: IS Used for IT Delivery and Support

- Lesson 6A: OSI
- Lesson 6B: TCP/IP Model
- Lesson 6C: TCP, UDP, ICMP and IP
- Lesson 6D: Routers, Switches and Hubs
- Lesson 6E: Firewalls and Wireless
- Lesson 6F: WAN Technologies

Module 7: Logical Assets Protection

- Lesson 7A: CIA
- Lesson 7B: RACI Roles and Responsibilities
- Lesson 7C: Managing Assets
- Lesson 7D: Information Classification
- Lesson 7E: Managing Risk
- Lesson 7F: Policies and Procedures
- Lesson 7G: Standards, Guidelines and Baselines
- Lesson 7H: Awareness, Training and Education

Module 8: Physical Security

- Lesson 8A: Practices for Environmental Protection
- Lesson 8B: Physical Authentication
- Lesson 8C: Procedures and Polices

Module 9: Business Continuity and Disaster Recovery

- Lesson 9A: BIA Policy, Roles and Teams
- Lesson 9B: Data Backups, Vaulting, Shadowing and Journaling
- Lesson 9C: Alternate Sites
- Lesson 9D: Emergency Responses and Notification Requirements
- Lesson 9E: BIA Tests

ISACA

CISM CERTIFIED INFORMATION SECURITY OFFICER

Course overview

CISM certification program was developed by the Information Systems Audit and Control Association (ISACA) for experienced Information security management professionals with work experience in developing and managing information security programs and who understand the programs relationship with the overall business goals. The CISM exam is offered three times a year (June, September, and December), consisting of 200 multiple-choice questions that cover the four CISM domains. The American National Standards Institute (ANSI) has accredited the CISM certification program under ISO/IEC 17024:2003, General Requirements for Bodies Operating Certification Systems of Persons.

WHAT YOU'LL LEARN

In-depth coverage of the four domains required to pass the CISM exam:

1. Information Security Governance
2. Information Risk Management and Compliance
3. Information Security Program Development and Management
4. Information Security Incident Management

WHATS INCLUDED:

- All Courseware
- Practice exams
- Exam Guidance

PREREQUISITES

5 YEARS OF WORK EXPERIENCE WITH AT LEAST 3 YEARS' EXPERIENCE IN 3 OR MORE OF THE FOLLOWING AREAS:

- INFORMATION SECURITY GOVERNANCE
- INFORMATION RISK MANAGEMENT
- INFORMATION SECURITY PROGRAM DEVELOPMENT
- INFORMATION SECURITY INCIDENT MANAGEMENT

WHO SHOULD ATTEND

- CISM certification program was developed by the Information Systems Audit and Control Association (ISACA) for experienced Information security management professionals with work experience in developing and managing information security programs and who understand the programs relationship with the overall business goals

FOLLOW UP COURSES:

Check with your Rep for a wide variety of options

Certifications:

CISM

OUTLINE & LABS

1. TESTING-TAKING TIPS AND STUDY TECHNIQUES

- Preparation for the CISM exam
- Submitting Required Paperwork
- Resources and Study Aids
- Passing the Exam the First Time

2. INFORMATION SECURITY GOVERNANCE

- Asset Identification
- Risk Assessment
- Vulnerability Assessments
- Asset Management

3. INFORMATION RISK MANAGEMENT

- Asset Classification and Ownership
- Structured Information Risk Assessment Process
- Business Impact Assessments
- Change Management

4. INFORMATION SECURITY PROGRAM DEVELOPMENT

- Information Security Strategy
- Program Alignment of Other Assurance Functions
- Development of Information Security Architectures
- Security Awareness, Training, and Education
- Communication and Maintenance of Standards, Procedures, and Other Documentation

- Change Control
- Lifecycle Activities
- Security Metrics

5. INFORMATION SECURITY PROGRAM MANAGEMENT

- Security Program Management Overview
- Planning
- Security Baselines
- Business Processes
- Security Program Infrastructure
- Lifecycle Methodologies
- Security Impact on Users
- Accountability
- Security Metrics
- Managing Resources

6. INCIDENT MANAGEMENT AND RESPONSE

- Response Management Overview
- Importance of Response Management
- Performing a Business Impact Analysis
- Developing Response and Recovery Plans
- The Incident Response Process
- Implementing Response and Recovery Plans
- Response Documentation
- Post-Event Reviews

7. REVIEW AND Q&A SESSION

- Final Review and Test Prep

INTERCONNECTING CISCO NETWORKING DEVICES, PART 1 (ICND1 V3.0)

Description section:

Course overview:

Interconnecting Cisco Networking Devices, Part 1 (ICND1) v3.0 is a five-day, instructor-led training course or a self-paced course that teaches learners how to install, operate, configure, and verify a basic IPv4 and IPv6 network, including configuring a LAN switch, configuring an IP router, managing network devices, and identifying basic security threats. Optionally, this course can be followed by the Interconnecting Cisco Networking Devices, Part 2 (ICND1) v3.0 course, which covers topics in more depth and teaches learners how to perform basic troubleshooting steps in enterprise branch office networks, preparingg learners for Cisco CCNA certification.

WHAT YOU'LL LEARN

Upon completing this course, the learner will be able to meet these overall objectives:

- Describe network fundamentals and build simple LANs
- Establish Internet connectivity
- Manage network device security
- Expand small- to medium-sized networks with WAN connectivity

- Describe IPv6 basics

This course includes:

- Cisco Authorized Digital course content

- Authorized Cisco CCSI Instructor

To participate in the hands-on labs in this class, you need to bring a laptop computer with the following:

- We recommend using at least a Pentium 4 or better and 1 GB of RAM or more.
- We recommend running Windows XP Professional SP3 or greater (Vista & Windows 7/8).
  Mac & Linux machines are also supported.
- **Browser Requirements:** Internet Explorer 10 or greater or Mozilla Firefox. (Safari and Mozilla Firefox for Mac OSX)
- All students are required to have administrator rights to their PCs and cannot be logged in to a domain using any Group Policies that will limit their machine's capabilities.
- If you do not have administrator rights to your PC, you at least need permissions to download, install, and run Cisco Any Connect Client.
- If you are participating in a WebEx event, it is highly recommended to take this class at a location that has bandwidth speeds at a minimum of 1 Mbps bandwidth speeds

PREREQUISITES

The knowledge and skills that a learner must have before attending this course are as follows:

- Basic computer literacy
- Basic PC Operating System navigation skills
- Basic Internet usage skills
- Basic IP addressing knowledge
- CO-NET+

WHO SHOULD ATTEND

Individuals seeking the Cisco CCENT certification, or Cisco CCNA Routing and Switching certification. The course is also appropriate for pre-sales and post-sales network engineers involved in the installation and support of enterprise branch office network.

Certifications: leads to CCNA and is part of Cisco Certified Entry Networking Technician (CCENT)

Cisco Certified Network Associate Wireless (CCNA Wireless)

Follow up classes

INTERCONNECTING CISCO NETWORK DEVICES PART 2 (ICND2)

IMPLEMENTING CISCO NETWORK SECURITY V3.0 (IINS)

OUTLINE & LABS

Course Introduction
The Course Introduction provides learners with the course objectives and prerequisite learner skills and knowledge. The Course Introduction presents the course flow diagram and the icons that are used in the course illustrations and figures. This course component also describes the curriculum for this course, providing learners with the information that they need to make decisions regarding their specific learning path.

- Overview
- Course Goal and Objectives
- Course Flow
- Your Training Curriculum
- Additional References

Module 1: Building a Simple Network
Objective: Describe network fundamentals and implement a simple LAN.

Lesson 1: Exploring the Functions of Networking
Objective: Identify the components of a computer network and describe their basic characteristics
This lesson includes these topics:

- What Is a Computer Network?
    - o   Objective: Define a network and describe examples of networks
- Physical Components of a Network

- o Objective: Identify common network components by function
- Characteristics of a Network
  - o Objective: List the characteristics of a network
- Physical vs. Logical Topologies
  - o Objective: Compare and contrast logical and physical topologies
- Interpreting a Network Diagram
  - o Objective: Interpret network diagrams
- Impact of User Applications on the Network
  - o Objective: Describe the impact of user applications on the network
- Challenge

Lesson 2: Understanding the Host-to-Host Communications Model
Objective: Understand the model of host-to-host communication
This lesson includes these topics:

- Introducing Host-to-Host Communications
  - o Objective: Identify the requirements of a host-to-host communication model
- OSI Reference Model
  - o Objective: Describe the OSI reference model
- TCP/IP Protocol Suite
  - o Objective: Describe the functions and purposes of the TCP/IP layers
- Peer-to-Peer Communications
  - o Objective: Describe how peer-to-peer communication works
- Encapsulation and De-Encapsulation
  - o Objective: Describe the process of encapsulation and de-encapsulation
- Challenge

Lesson 3: Introducing LANs
Objective: Describe LANs and the role of switches within LANs
This lesson includes these topics:

- Local Area Networks
  - o Objective: Define LAN
- LAN Components
  - o Objective: Identify the components of a LAN
- Need for Switches
  - o Objective: Identify the need for the switches in a LAN
- Switches

- o Objective: List the characteristics and features of Switches
- Challenge

Lesson 4: Operating Cisco IOS Software
Objective: Describe the features and functions of the Cisco IOS Software
This lesson includes these topics:

- Cisco IOS Software Features and Functions
  - o Objective: List the features and functions of Cisco IOS Software
- Cisco IOS CLI Functions
  - o Objective: Lists the functions and usage of Cisco CLI.
- Cisco IOS Software Modes
  - o Objective: IOS software modes on Cisco devices.
- Discovery 1: Get Started with Cisco CLI
  - o Objective: This is the first lab lesson in the course and it will help you to get familiar with Cisco CLI.
  - o Topology
  - o Job Aid
  - o Task 1: Navigate Between EXEC Modes
  - o Task 2: Explore CLI Help
  - o Task 3: Manage Cisco IOS Configuration
  - o Task 4: Improve User Experience in CLI
- Challenge

Lesson 5: Starting a Switch
Objective: Install a switch and perform the initial configuration
This lesson includes these topics:

- Switch Installation
  - o Objective: Identify physical installation requirements
- Switch LED Indicators
  - o Objective: Identify the conditions that are reflected by the LEDs on switches
- Connecting to a Console Port
  - o Objective: Connect to a switch console port
- Basic Show Commands and Information
  - o Objective: List fundamental show commands.
- Discovery 2: Perform Basic Switch Configuration
  - o Objective: Configure switch from command line and verify the configuration.

- o Topology
- o Job Aid
- o Task 1: Configure a Switch from the Command Line
- o Task 2: Verify the Switch Initial Startup Status
- Challenge
  - o Challenge 1: Implementing the Initial Switch Configuration
  - o Objective: Perform basic switch configuration based on the challenge scenario.
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure
- Command List

Lesson 6: Understanding Ethernet and Switch Operation
Objective: Describe Ethernet as the network access layer of TCP/IP and describe the operation of switches
This lesson includes these topics:

- Ethernet LAN Connection Media
  - o Objective: Describe the types of Ethernet LAN connection media
- Ethernet Frame Structure
  - o Objective: Describe the fields of an Ethernet frame
- MAC Addresses
  - o Objective: Define the structure and function of MAC addresses
- Frame Switching
  - o Objective: Explain the basic concept of switching.
- Discovery 3: Observe How a Switch Operates
  - o Objective: Describe how switches operate and build CAM table
  - o Topology
  - o Job Aid
  - o Task 1: Observe How a Switch Operates
- Duplex Communication
  - o Objective: Compare half-duplex and full-duplex operation and also configure it on an interface.
- Challenge

Lesson 7: Troubleshooting Common Switch Media Issues
Objective: Identify and resolve common switched network issues
This lesson includes these topics:

- Troubleshooting Methods
  - Objective: Describe the Troubleshooting methods
- Troubleshooting Tools
  - Objective: Describe common Troubleshooting Tools.
- Troubleshooting Common Switch Media Issues
  - Objective: Identify common switched network media issues
- Troubleshooting Common Switch Port Issues
  - Objective: Identify common access port issues
- General Troubleshooting Process
  - Objective: How to troubleshoot duplex issues.
- Discovery 4: Troubleshoot Switch Media and Port Issues
  - Objective: Troubleshoot Switch Media and Port Issues
  - Topology
  - Job Aid
  - Task 1: Troubleshoot Port Issues
- Challenge

Module 2: Establishing Internet Connectivity
Objective: Establish Internet connectivity

Lesson 1: Understanding the TCP/IP Internet Layer
Objective: Describe IPv4 and its addressing scheme
This lesson includes these topics:

- Internet Protocol
  - Objective: List the characteristics of IP
- IPv4 Address Representation
  - Objective: Describe the components of an IPv4 address
- IPv4 Header Address Fields
  - Objective: Identify the fields within the IPv4 header
- Decimal and Binary Systems
  - Objective: Describe the decimal and binary number systems
- Decimal-to-Binary Conversion
  - Objective: Convert a decimal number to a binary number
- IP Address Classes
  - Objective: List the classes of IPv4 addresses
- Reserved IPv4 Addresses

- o Objective: Describe reserved IPv4 addresses
- Private vs. Public IP Addresses
  - o Objective: Describe and differentiate between Public and Private addresses
- Domain Name System
  - o Objective: Define the function of DNS
- Verifying the IPv4 Address of a Host
  - o Objective: Verify the IPv4 address of a host
- Challenge

Lesson 2: Understanding IP Addressing and Subnets
Objective: Describe subnets, subnetting, and the role of subnet masks
This lesson includes these topics:

- Subnets
  - o Objective: Describe the purposes and functions of subnets and their addressing schemes
- Subnet Masks
  - o Objective: Explain the role of a subnet mask
- Implementing Subnetting: Borrowing Bits
  - o Objective: Understand how subnetting is implemented.
- Implementing Subnetting: Determing the Addressing Scheme
  - o Objective: Understand subnetting
- Benefits of VLSM and Implementing VLSM
  - o Objective: Describe the role of VLSM and also how to implement it.
- Challenge

Lesson 3: Understanding the TCP/IP Transport Layer
Objective: Describe the TCP/IP transport layer
This lesson includes these topics:

- TCP/IP Transport Layer Functions
  - o Objective: Explain the purpose and major functions of the TCP/IP transport layer
- Reliable vs. Best-Effort Transport
  - o Objective: Contrast connection-oriented transport with connectionless transport
- TCP vs. UDP Analogy
  - o Objective: Explain the basic difference between TCP and UDP
- TCP Characteristics
  - o Objective: Explain the characteristics of TCP in brief.

- UDP Characteristics
  - Objective: Describe the characteristics of UDP in brief.
- TCP/IP Applications
  - Objective: List the common applications that are provided by TCP/IP
- Discovery 5: Inspect TCP/IP Applications
  - Objective: List the common applications that are provided by TCP/IP
  - Topology
  - Job Aid
  - Task 1: Inspect TCP/IP Applications
- Challenge

Lesson 4: Exploring the Functions of Routing

Objective: Define the role, components and function of a Router Understand how a Routing Table conveys information Understand how a Router chooses a path or route Understand how Dynamic Routing protocols calculate and communicate routing information

This lesson includes these topics:

- Role of a Router
  - Objective: Describe the role of a router in the IP packet delivery process
- Router Components
  - Objective: Describe the physical characteristics of a router
- Router Function
  - Objective: Describe the functions of a router
- Routing Table
  - Objective: Describe the components of routing table
- Dynamic Routing Protocol
  - Objective: Describe the function of dynamic routing protocols
- Path Determination
  - Objective: Describe router path determination.
- Route Selection
  - Objective: Describe how router selects the best path
- Challenge

Lesson 5: Configuring a Cisco Router

Objective: Implement basic configuration on a Cisco router
This lesson includes these topics:

- Initial Router Setup
  - Objective: Describe router startup

- Configuring Router Interfaces
  - Objective: Describe how to configuring router interfaces
- IP Addresses on Router Interfaces
  - Objective: Explain how to configure IP address on an interface and why.
- Checking Interface Configuration and Status
  - Objective: Explain how to check interface configuration.
- Discovery 6: Start with Cisco Router Configuration
  - Objective: Perform basic Cisco Router configuration
  - Topology
  - Job Aid
  - Task 1: Configure an IP Address on the Router Interfaces
  - Task 2: Verify Interface Configuration and Status
- Exploring Connected Devices
  - Objective: Describe the need for a network discovery protocol.
- Using Cisco Discovery Protocol
  - Objective: Explain how CDP operates.
- Discovery 7: Configure Cisco Discovery Protocol
  - Objective: Configure and verify CDP and LLDP.
  - Topology
  - Job Aid
  - Task 1: Discover Neighbors Using Cisco Discovery Protocol
- Configuring LLDP
  - Objective: Describe LLDP configuration
- Challenge
  - Challenge 2: Implementing the Initial Router Configuration
  - Objective: Learn to configure basic router settings
  - Topology
  - Job Aid
  - Task 1: Evaluation Lab Procedure
- Command List

Lesson 6: Exploring the Packet Delivery Process
Objective: Understand host-to-host communications across switches and routers
This lesson includes these topics:

- Address Resolution Protocol
  - Objective: Explain the role of ARP

- Default Gateways
    - Objective: Elaborate what default gateway is and why it is used.
- Discovery 8: Configure Default Gateway
    - Objective: Describe how end systems use subnet masks and default gateways
    - Topology
    - Job Aid
    - Task 1: Configure Default Gateway
- Host-to-Host Packet Delivery
    - Objective: Describe the host-to-host packet delivery
- Role of a Switch in Packet Delivery
    - Objective: Describe the host-to-host packet delivery process through a switch
- Discovery 9: Exploration of Packet Forwarding
    - Objective: This discovery will show how packet forwarding happens through devices by observing through show commands and debugs.
    - Topology
    - Job Aid
    - Task 1: Exploration of Packet Forwarding
- Troubleshooting Common Problems Associated with IP Addressing
    - Objective: Describe the common common troubleshooting tools.
- Challenge

Lesson 7: Enabling Static Routing
Objective: Describe the operation, benefits, and limitations of static routing
This lesson includes these topics:

- Routing Operation
    - Objective: Describe the basic characteristics of routing operations
- Static and Dynamic Routing Comparison
    - Objective: Explain the differences between static and dynamic routing
- When to Use Static Routing
    - Objective: Explain when to use static routing
- Static Route Configuration
    - Objective: Describe how to configure static route configuration
- Default Routes
    - Objective: Describe how to configure default route configuration
- Verifying the Static Route Configuration
    - Objective: Describe how to verify static route configuration

- Verifying the Default Route Configuration
  - Objective: Describe how to verify default route configuration
- Discovery 10: Configure and Verify Static Routes
  - Objective: Configure static routes
  - Topology
  - Job Aid
  - Task 1: Verify Devices Reachability
  - Task 2: Configure and Verify Static Routes
  - Task 3: Demonstrate Static Route Drawback
  - Task 4: Configure and Verify the Backup Static Route
  - Task 5: Configure and Verify the Default Route
- Challenge
  - Challenge 3: Implementing Static Routing
  - Objective: Learn to configure and use static routes.
  - Topology
  - Job Aid
  - Task 1: Evaluation Lab Procedure
- Command List

Lesson 8: Learning the Basics of ACL
Objective: Describe the operation of ACLs and their applications in the network
This lesson includes these topics:

- ACL Overview
  - Objective: Describe what ACLs are
- ACL Operation
  - Objective: Explain how ACLs operate
- ACL Wildcard Masking
  - Objective: Describe ACL wildcard masking
- Wildcard Bit Mask Abbreviations
  - Objective: Describe ACL wildcard bit mask abbreviations
- Types of ACLs
  - Objective: Describe types of ACLs
- Testing an IP Packet Against a Numbered Standard Access List
  - Objective: Describe how to test an IP packet against a numbered standard access list
- Configuring Standard IPv4 ACLs

- o Objective: Explain numbered IPv4 ACLs.
- Discovery 11: Configure and Verify ACLs
  - o Objective: Configure named and standard ACLs.
  - o Topology
  - o Job Aid
  - o Task 1: Configure Numbered Standard IPv4 ACLs
  - o Task 2: Filter Traffic Using ACLs
- Using ACLs to Filter Network Traffic
  - o Objective: Describe traffic filtering with ACLs
- Applying ACLs to Interfaces
  - o Objective: Apply an ACL to an interface
- Configuring Named ACLs
  - o Objective: Configure and edit named IPv4 ACLs
- Challenge
  - o Challenge 4: Implementing Basic Numbered and Named ACLs
  - o Objective: Learn to configure standard and named ACLs
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure
- Command List

Lesson 9: Enabling Internet Connectivity
Objective: Configure Internet access using DHCP clients, NAT, and PAT on Cisco routers
This lesson includes these topics:

- Demarcation Point
  - o Objective: Explain the demarcation point
- Provider-Assigned IP Addresses
  - o Objective: Expain DHCP and static addressing.
- Public vs. Private IPv4 Addresses
  - o Objective:
- Discovery 12: Configure a Provider-Assigned IP Address
  - o Objective: Configure a Static Provider Assigned IP address and Configuring DHCP Client
  - o Topology
  - o Job Aid
  - o Task 1: Configure a Provider-Assigned IP Address

- Introducing NAT
  - Objective: Describe the features and benefits of NAT
- Types of Addresses in NAT
  - Objective: Describe types of NAT addresses
- Types of NAT
  - Objective: Describe types of NAT
- Understanding Static NAT
  - Objective: Explain static NAT.
- Configuring and Verifying Static NAT
  - Objective: Explain how to configure and verify static NAT.
- Discovery 13: Configure Static NAT
  - Objective: Configure static NAT and explain its operation
  - Topology
  - Job Aid
  - Task 1: Configure Static NAT
- Understanding Dynamic NAT
  - Objective: Explain dynamic NAT.
- Configuring and Verifying Dynamic NAT
  - Objective: Explain how to configure dynamic NAT.
- Understanding PAT
  - Objective: Introduce and explain PAT.
- Configuring and Verifying PAT
  - Objective: Explain how to configure and verify PAT.
- Discovery 14: Configure Dynamic NAT and PAT
  - Objective: Understand how dynamic NAT works and also to configure it
  - Topology
  - Job Aid
  - Task 1: Configure Dynamic NAT and PAT
- Troubleshooting NAT
  - Objective: Illustrate how to troubleshoot NAT.
- Discovery 15: Troubleshoot NAT
  - Objective: Troubleshoot NAT related issues.
  - Topology
  - Job Aid
  - Task 1: Troubleshoot NAT

- Challenge
    - o Challenge 5: Implementing PAT
    - o Objective: PAT configuration and verification
    - o Topology
    - o Job Aid
    - o Task 1: Evaluation Lab Procedure
- Command List

Module 3: Summary Challenge
Objective: Configure and troubleshoot topics learn in Module 1 and Module 2.

Lesson 1: Establish Internet Connectivity
Objective: Establish internet connectivity.
This lesson includes these topics:

- Challenge
    - o Challenge 6: Summary Challenge Lab: 1
    - o Objective: Summary Challenge lab on topics from Mod 1 and Mod 2.
    - o Topology
    - o Job Aid
    - o Task 1: Evaluation Lab Procedure

Lesson 2: Troubleshoot Internet Connectivity
Objective: Troubleshoot internet connectivity.
This lesson includes these topics:

- Challenge
    - o Challenge 7: Summary Challenge Lab: 2
    - o Objective: Summary Challenge lab on topics from Mod 1 and Mod 2.
    - o Topology
    - o Job Aid
    - o Task 1: Evaluation Lab Procedure

Module 4: Building a Medium-Sized Network
Objective: Expand a small network to a medium-sized network with routing enabled.

Lesson 1: Implementing VLANs and Trunks
Objective: Implement and verify VLANs and trunking
This lesson includes these topics:

- Enterprise Network Design
    - o Objective: Describe the enterprise network design.

- Issues in a Poorly Designed Network
  - Objective: Describe the issues in poorly designed LANs
- VLAN Introduction
  - Objective: Describe the purpose and functions of VLANs
- Creating a VLAN
  - Objective: Explains how to create a VLAN.
- Assigning a Port to a VLAN
  - Objective: Describes how to assign a Port to a VLAN
- Trunking with 802.1Q
  - Objective: Define the purpose and function of trunking
- Configuring an 802.1Q Trunk
  - Objective: Describe how to configure an 802.1Q Trunk
- Discovery 16: Configure VLAN and Trunk
  - Objective: Configure, verify and troubleshoot VLANs and trunks.
  - Topology
  - Job Aid
  - Task 1: Configure VLAN and Trunk
- VLAN Design Consideration
  - Objective: Describe VLAN design and creation guidelines
- Physical Redundancy in a LAN
  - Objective: Describe how redundancy in a network can cause broadcast loops and describe a solution to this problem
- Challenge
  - Challenge 8: Troubleshooting VLANs and Trunk
  - Objective: Configure and troubleshoot VLANs on multiple switches and configure routing of the traffic between them.
  - Topology
  - Job Aid
  - Task 1: Evaluation Lab Procedure
- Command List

Lesson 2: Routing Between VLANs
Objective: Describe the application and configuration of inter-VLAN routing
This lesson includes these topics:

- Purpose of Inter-VLAN Routing
  - Objective: Describe the need for inter-VLAN routing

- Options for Inter-VLAN Routing
  - Objective: Describe options for inter-VLAN routing
- Discovery 17: Configure a Router on a Stick
  - Objective: Configure Router on a Stick.
  - Topology
  - Job Aid
  - Task 1: Configure a Router with a Trunk Link
- Challenge
  - Challenge 9: Implement Multiple VLANs and Basic Routing Between the VLANs
  - Objective: Test your learning on VLANs and Inter-VLAN routing
  - Topology
  - Job Aid
  - Task 1: Evaluation Lab Procedure
- Command List

Lesson 3: Using a Cisco IOS Network Device as a DHCP Server
Objective: Configure a Cisco IOS DHCPv4 server on a Cisco router and switch
This lesson includes these topics:

- Need for a DHCP Server
  - Objective: Describe the need for dynamic host IP address assignment
- Understanding DHCP

  Note This topic focuses on DHCP address allocation. Students should already be familiar with general DHCP properties and other DHCP allocation methods.

  - Objective: Describe DHCP operation
- Configuring a DHCP Server
  - Objective: Configure DHCP server
- Discovery 18: Configure a Cisco Router as a DHCP Server
  - Objective: Configure and verify Cisco routers as DHCP servers.
  - Topology
  - Job Aid
  - Task 1: Configure a Cisco Router as a DHCP Server
- Understanding DNS
  - Objective: Describe how DNS look up works
  - Discovery 19: Troubleshoot DHCP Issues
  - Objective: Troubleshoot DHCP and DNS issues.

- - - Topology
  - - Job Aid
  - - Task 1: Troubleshooting DHCP Issues
- Challenge
  - - Challenge 10: Implementing a DHCP Server in on a Cisco IOS Device.
  - - Objective: Learn to configure Cisco Router as DHCP server
  - - Topology
  - - Job Aid
  - - Task 1: Evaluation Lab Procedure
- Command List

Lesson 4: Implementing RIPv2

Objective: Describe the operation and configuration of RIPv2.

This lesson includes these topics:

- Overview of Routing Protocols
  - - Objective: Describe the need for dynamic routing protocols
- Distance Vector and Link-State Routing Protocols
  - - Objective: Describe distance vector and link-state routing protocols
- Understanding RIPv2
  - - Objective: Describe RIPv2
- Configure RIPv2
  - - Objective: Describe how to configure RIPv2
- Verify RIPv2
  - - Objective: Describe how to verify RIPv2
- Discovery 20: Configure and Verify RIPv2
  - - Objective: Configure and verify RIPv2
  - - Topology
  - - Job Aid
  - - Task 1: Configure and Verify RIPv2
  - - Task 2: Adjust RIP Timers
  - - Task 3: Disable RIP Auto Summary
  - - Task 4: Configure a RIP Passive Interface
  - - Task 5: Generate a Default RIP Route
- Discovery 21: Troubleshoot RIPv2
  - - Objective: Troubleshoot RIPv2
  - - Topology

- o Job Aid
- o Task 1: Troubleshoot RIPv2
- Challenge
    - o Challenge 11: Implementing RIPv2
    - o Objective: Configure and troubleshoot RIPv2.
    - o Topology
    - o Job Aid
    - o Task 1: Evaluation Lab Procedure
- Command List

Module 5: Network Device Management and Security
Objective: Configure, manage and monitor Cisco devices.

Lesson 1: Securing Administrative Access
Objective: Implement a basic security configuration
This lesson includes these topics:

- Network Device Security Overview
    - o Objective: List the actions that are required to secure a network device
- Securing Access to Privileged EXEC Mode
    - o Objective: Secure access to privileged EXEC mode
- Securing Console Access
    - o Objective: Secure console access to a network device
- Securing Remote Access
    - o Objective: Secure remote access to a network device
- Discovery 22: Enhance Security of Initial Configuration
    - o Objective: Learn basic configuration to secure initial config.
    - o Topology
    - o Job Aid
    - o Task 1: Secure Access to Privileged EXEC Mode
    - o Task 2: Secure Console and Remote Access
    - o Task 3: Enable SSH
- Limiting Remote Access with ACLs
    - o Objective: Limit remote access with an ACL
- Configuring the Login Banner
    - o Objective: Configure the login banner
- Discovery 23: Limit Remote Access Connectivity

- Objective: Learn how to enable and secure remote access connectivity
  - Topology
  - Job Aid
  - Task 1: Limit Remote Access with ACLs
  - Task 2: Configure the Login and EXEC Banners
- Challenge
  - Challenge 12: Securing Device Administrative Access
  - Objective: Securing access to Devices.
  - Topology
  - Job Aid
  - Task 1: Evaluation Lab Procedure
- Command List

Lesson 2: Implementing Device Hardening
Objective: Implement basic steps to harden network devices
This lesson includes these topics:

- Securing Unused Ports
  - Objective: Secure unused ports
- Port Security
  - Objective: Describe port security
- Configuring Port Security
  - Objective: Configure port security
- Verifying Port Security
  - Objective: Verify port security
- Discovery 24: Configure and Verify Port Security
  - Objective: Learn to configure Port security
  - Topology
  - Job Aid
  - Task 1: Configure and Verify Port Security
- Disabling Unused Services
  - Objective: Disable unused services
- Network Time Protocol
  - Objective: Describe NTP
- Configuring NTP
  - Objective: Configure basic NTP
- Verifying NTP

- o Objective: Verify NTP
- Discovery 25: Configure and Verify NTP
  - o Objective: Configure and verify NTP in Client Server mode.
  - o Topology
  - o Job Aid
  - o Task 1: Configure and Verify NTP
- Challenge
  - o Challenge 13: Implementing Device Hardening
  - o Objective: Learn to configure NTP and port security
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure
- Command List

Lesson 3: Configuring System Message Logging
Objective: Configure System Message Logging
This lesson includes these topics:

- Syslog Overview
  - o Objective: Explain why syslog is used
- Syslog Message Format
  - o Objective: Describe the format of syslog messages
- Syslog Configuration
  - o Objective: Configure syslog on a Cisco device
- Discovery 26: Configure Syslog
  - o Objective: Describe Syslog Configuration
  - o Topology
  - o Job Aid
  - o Task 1: Configure Syslog
- Challenge
  - o Challenge 14: Configuring System Message Logging
  - o Objective: Configure and verify System message logging.
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure
- Command List

Lesson 4: Managing Cisco Devices

Objective: Describe the management of Cisco devices

This lesson includes these topics:

- Router Internal Components
    - Objective: Describe the major internal components of a Cisco router
- ROM Functions
    - Objective: Describe the functions of ROM in a Cisco router
- Stages of the Router Power-On Boot Sequence
    - Objective: Describe the sequence of events that occurs during a router boot
- Configuration Register
    - Objective: Describe how to display the boot information in the configuration register
- Locating Cisco IOS Image Files
    - Objective: Describe the process of locating Cisco IOS images
- Loading Cisco IOS Image Files
    - Objective: Describe the process of loading Cisco IOS images
- Loading Cisco IOS Configuration Files
    - Objective: Describe the process of loading Cisco IOS configuration files
- Cisco IOS Integrated File System and Devices
    - Objective: Describe the file systems that are used by a Cisco router
- Managing Cisco IOS Images
    - Objective: Describe why it is important to create a backup of Cisco IOS images and configuration files
- Deciphering Cisco IOS Image Filenames
    - Objective: Describe how to decipher Cisco IOS image filenames
- Managing Device Configuration Files
    - Objective: Describe the configuration files and their location
- Password Recovery
    - Objective: Describe how to perform a password recovery on a Cisco router
- Challenge

Lesson 5: Licensing

Objective: Understand licensing under Cisco IOS 15. In this lesson we can use an EAI to demonstrate license installation and verification.

This lesson includes these topics:

- Licensing Overview

- o Objective: Explain Cisco IOS image licensing
  - Licensing Verification
    - o Objective: Explain how a current version of the license can be identified
  - Permanent License Installation
    - o Objective: Explain how to install a permanent license
  - Evaluation License Installation
    - o Objective: Explain how to install an evaluation license
  - Backing Up the License
    - o Objective: Explain how to back up a license
  - Uninstalling the License
    - o Objective: Explain how to uninstall a license
  - Cisco Smart Software Manager
    - o Objective: Descrive Cisco Smart Software Manager
  - Challenge

Module 6: Summary Challenge

Objective: Configure and troubleshoot a medium sized network.

Lesson 1: Implementing a Medium-Sized Network
This lesson includes these topics:

- Challenge
  - o Challenge 15: Summary Challenge Lab: 3
  - o Objective: Based on Mod 3 and Mod 4 topics a summary challenge lab to be created.
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure

Lesson 2: Troubleshooting a Medium-Sized Network
This lesson includes these topics:

- Challenge
  - o Challenge 16: Summary Challenge Lab: 4
  - o Objective: Based on Mod 3 and Mod 4 topics a summary challenge lab to be created.
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure

Module 7: Introducing IPv6
Objective: Describe IPv6 basics

Lesson 1: Introducing Basic IPv6
Objective: Describe IPv6 main features, addresses.
This lesson includes these topics:

- IPv4 Addressing Exhaustion Workarounds
    - Objective: Identify issues in IPv4
- IPv6 Features
    - Objective: Identify the main IPv6 features
- IPv6 Addresses
    - Objective: Describe IPv6 addresses and address types
- IPv6 Address Scopes and Prefixes
    - Objective: Describes the IPv6 unicast addresses.
- IPv6 Address Allocation
    - Objective: Describe manual address assignment, stateless autoconfiguration, and DHCPv6
- Challenge

Lesson 2: Understanding IPv6 Operation
Objective: Describe IPv6 operations and basic IPv6 configuration.
This lesson includes these topics:

- Comparison of IPv4 and IPv6 Headers
    - Objective: Compare the IPv4 and IPv6 header
- Internet Control Message Protocol Version 6
    - Objective: Describe ICMPv6
- Neighbor Discovery
    - Objective: Describe the neighbor discovery process and mapping from IPv6 addresses to Layer 2 addresses
- Stateless Address Autoconfiguration
    - Objective: Describe and configure stateless autoconfiguration
- Discovery 27: Configure Basic IPv6 Connectivity
    - Objective: Basic IPv6 commands
    - Topology
    - Job Aid
    - Task 1: Configure IPv6 Addresses
    - Task 2: Configure IPv6 Stateless Autoconfiguration

- Challenge

Lesson 3: Configuring IPv6 Static Routes

Objective: Identify routing protocols for IPv6

This lesson includes these topics:

- Routing for IPv6

    - Objective: Describe routing types for IPv6

- Configuring IPv6 Static Routes

    - Objective: Describe how to configure and verify IPv6 static routes

- Discovery 28: Configure IPv6 Static Routes

    - Objective: Configure and verify IPv6 static routes.

    - Topology

    - Job Aid

    - Task 1: Configure IPv6 Default Routes

    - Task 2: Configure IPv6 Static Routes

- Challenge

    - Challenge 17: Implement IPv6 Static Routing

    - Objective: Troubleshoot IPv6 routing.

    - Topology

    - Job Aid

    - Task 1: Evaluation Lab Procedure

- Command List

INTERCONNECTING CISCO NETWORKING DEVICES, PART 2

Description section:

Course overview:

Interconnecting Cisco Networking Devices, Part 2 (ICND2) v3.0 is a five-day, instructor-led training course or a self paced course that teaches learners how to perform basic troubleshooting steps in enterprise branch office networks, preparing learners for Cisco CCNA certification.

WHAT YOU'LL LEARN

Upon completing this course, the learner will be able to meet these overall objectives:

- Install, operate, and troubleshoot a medium-sized network, including connecting to a WAN and implementing network security.
- Describe the effects of new technologies such as IoE, IoT, IWAN, and SDN on network evolution.

This course includes:

- Cisco Authorized Digital course content

- Authorized Cisco CCSI Instructor

To participate in the hands-on labs in this class, you need to bring a laptop computer with the following:

- We recommend using at least a Pentium 4 or better and 1 GB of RAM or more.
- We recommend running Windows XP Professional SP3 or greater (Vista & Windows 7/8).
  Mac & Linux machines are also supported.
- **Browser Requirements:** Internet Explorer 10 or greater or Mozilla Firefox. (Safari and Mozilla Firefox for Mac OSX)
- All students are required to have administrator rights to their PCs and cannot be logged in to a domain using any Group Policies that will limit their machine's capabilities.
- If you do not have administrator rights to your PC, you at least need permissions to download, install, and run Cisco Any Connect Client.
- If you are participating in a WebEx event, it is highly recommended to take this class at a location that has bandwidth speeds at a minimum of 1 Mbps bandwidth speeds

PREREQUISITES

The knowledge and skills that a learner must have before attending this course are as follows:

INTERCONNECTING CISCO NETWORK DEVICES PART 1 (ICND1) OR NETWORK+

- Understand network fundamentals
- Implement local area networks
- Implement Internet connectivity
- Manage network device security

- Implement WAN connectivity
- Implement basic IPv6 connectivity

- **Target Candidate:** Individuals seeking the Cisco CCNA Routing and Switching certification. The course is also appropriate for pre-sales and post-sales network engineers involved in the installation and support of enterprise branch office networks.

Cisco Certified Network Associate Wireless (CCNA Wireless)

Follow up classes

IMPLEMENTING CISCO IP ROUTING V2.0 (ROUTE)

IMPLEMENTING CISCO IP SWITCHED NETWORKS V2.0 (SWITCH)

TROUBLESHOOTING AND MAINTAINING CISCO IP NETWORKS V2.0 (TSHOOT)

OUTLINE & LABS

Course Introduction
The Course Introduction provides learners with the course objectives and prerequisite learner skills and knowledge. The Course Introduction presents the course flow diagram and the icons that are used in the course illustrations and figures. This course component also describes the curriculum for this course, providing learners with the information that they need to make decisions regarding their specific learning path.

- Overview
- Course Goal and Objectives
- Course Flow
- Your Training Curriculum
- Additional References

Module 1: Building a Simple Network
Objective: Describe network fundamentals and implement a simple LAN.

Lesson 1: Exploring the Functions of Networking

Objective: Identify the components of a computer network and describe their basic characteristics

This lesson includes these topics:

- What Is a Computer Network?
    - Objective: Define a network and describe examples of networks
- Physical Components of a Network
    - Objective: Identify common network components by function
- Characteristics of a Network
    - Objective: List the characteristics of a network
- Physical vs. Logical Topologies
    - Objective: Compare and contrast logical and physical topologies
- Interpreting a Network Diagram
    - Objective: Interpret network diagrams
- Impact of User Applications on the Network
    - Objective: Describe the impact of user applications on the network
- Challenge

Lesson 2: Understanding the Host-to-Host Communications Model

Objective: Understand the model of host-to-host communication

This lesson includes these topics:

- Introducing Host-to-Host Communications
    - Objective: Identify the requirements of a host-to-host communication model
- OSI Reference Model
    - Objective: Describe the OSI reference model
- TCP/IP Protocol Suite
    - Objective: Describe the functions and purposes of the TCP/IP layers
- Peer-to-Peer Communications
    - Objective: Describe how peer-to-peer communication works
- Encapsulation and De-Encapsulation
    - Objective: Describe the process of encapsulation and de-encapsulation
- Challenge

Lesson 3: Introducing LANs

Objective: Describe LANs and the role of switches within LANs

This lesson includes these topics:

- Local Area Networks
  - Objective: Define LAN
- LAN Components
  - Objective: Identify the components of a LAN
- Need for Switches
  - Objective: Identify the need for the switches in a LAN
- Switches
  - Objective: List the characteristics and features of Switches
- Challenge

Lesson 4: Operating Cisco IOS Software
Objective: Describe the features and functions of the Cisco IOS Software
This lesson includes these topics:

- Cisco IOS Software Features and Functions
  - Objective: List the features and functions of Cisco IOS Software
- Cisco IOS CLI Functions
  - Objective: Lists the functions and usage of Cisco CLI.
- Cisco IOS Software Modes
  - Objective: IOS software modes on Cisco devices.
- Discovery 1: Get Started with Cisco CLI
  - Objective: This is the first lab lesson in the course and it will help you to get familiar with Cisco CLI.
  - Topology
  - Job Aid
  - Task 1: Navigate Between EXEC Modes
  - Task 2: Explore CLI Help
  - Task 3: Manage Cisco IOS Configuration
  - Task 4: Improve User Experience in CLI
- Challenge

Lesson 5: Starting a Switch
Objective: Install a switch and perform the initial configuration
This lesson includes these topics:

- Switch Installation
  - Objective: Identify physical installation requirements
- Switch LED Indicators

- o Objective: Identify the conditions that are reflected by the LEDs on switches
- Connecting to a Console Port
  - o Objective: Connect to a switch console port
- Basic Show Commands and Information
  - o Objective: List fundamental show commands.
- Discovery 2: Perform Basic Switch Configuration
  - o Objective: Configure switch from command line and verify the configuration.
  - o Topology
  - o Job Aid
  - o Task 1: Configure a Switch from the Command Line
  - o Task 2: Verify the Switch Initial Startup Status
- Challenge
  - o Challenge 1: Implementing the Initial Switch Configuration
  - o Objective: Perform basic switch configuration based on the challenge scenario.
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure
- Command List

Lesson 6: Understanding Ethernet and Switch Operation

Objective: Describe Ethernet as the network access layer of TCP/IP and describe the operation of switches

This lesson includes these topics:

- Ethernet LAN Connection Media
  - o Objective: Describe the types of Ethernet LAN connection media
- Ethernet Frame Structure
  - o Objective: Describe the fields of an Ethernet frame
- MAC Addresses
  - o Objective: Define the structure and function of MAC addresses
- Frame Switching
  - o Objective: Explain the basic concept of switching.
- Discovery 3: Observe How a Switch Operates
  - o Objective: Describe how switches operate and build CAM table
  - o Topology
  - o Job Aid
  - o Task 1: Observe How a Switch Operates

- Duplex Communication
  - Objective: Compare half-duplex and full-duplex operation and also configure it on an interface.
- Challenge

Lesson 7: Troubleshooting Common Switch Media Issues
Objective: Identify and resolve common switched network issues
This lesson includes these topics:

- Troubleshooting Methods
  - Objective: Describe the Troubleshooting methods
- Troubleshooting Tools
  - Objective: Describe common Troubleshooting Tools.
- Troubleshooting Common Switch Media Issues
  - Objective: Identify common switched network media issues
- Troubleshooting Common Switch Port Issues
  - Objective: Identify common access port issues
- General Troubleshooting Process
  - Objective: How to troubleshoot duplex issues.
- Discovery 4: Troubleshoot Switch Media and Port Issues
  - Objective: Troubleshoot Switch Media and Port Issues
  - Topology
  - Job Aid
  - Task 1: Troubleshoot Port Issues
- Challenge

Module 2: Establishing Internet Connectivity
Objective: Establish Internet connectivity

Lesson 1: Understanding the TCP/IP Internet Layer
Objective: Describe IPv4 and its addressing scheme
This lesson includes these topics:

- Internet Protocol
  - Objective: List the characteristics of IP
- IPv4 Address Representation
  - Objective: Describe the components of an IPv4 address
- IPv4 Header Address Fields
  - Objective: Identify the fields within the IPv4 header

- Decimal and Binary Systems
  - Objective: Describe the decimal and binary number systems
- Decimal-to-Binary Conversion
  - Objective: Convert a decimal number to a binary number
- IP Address Classes
  - Objective: List the classes of IPv4 addresses
- Reserved IPv4 Addresses
  - Objective: Describe reserved IPv4 addresses
- Private vs. Public IP Addresses
  - Objective: Describe and differentiate between Public and Private addresses
- Domain Name System
  - Objective: Define the function of DNS
- Verifying the IPv4 Address of a Host
  - Objective: Verify the IPv4 address of a host
- Challenge

Lesson 2: Understanding IP Addressing and Subnets
Objective: Describe subnets, subnetting, and the role of subnet masks
This lesson includes these topics:

- Subnets
  - Objective: Describe the purposes and functions of subnets and their addressing schemes
- Subnet Masks
  - Objective: Explain the role of a subnet mask
- Implementing Subnetting: Borrowing Bits
  - Objective: Understand how subnetting is implemented.
- Implementing Subnetting: Determing the Addressing Scheme
  - Objective: Understand subnetting
- Benefits of VLSM and Implementing VLSM
  - Objective: Describe the role of VLSM and also how to implement it.
- Challenge

Lesson 3: Understanding the TCP/IP Transport Layer
Objective: Describe the TCP/IP transport layer
This lesson includes these topics:

- TCP/IP Transport Layer Functions

- o Objective: Explain the purpose and major functions of the TCP/IP transport layer
- Reliable vs. Best-Effort Transport
  - o Objective: Contrast connection-oriented transport with connectionless transport
- TCP vs. UDP Analogy
  - o Objective: Explain the basic difference between TCP and UDP
- TCP Characteristics
  - o Objective: Explain the characteristics of TCP in brief.
- UDP Characteristics
  - o Objective: Describe the characteristics of UDP in brief.
- TCP/IP Applications
  - o Objective: List the common applications that are provided by TCP/IP
- Discovery 5: Inspect TCP/IP Applications
  - o Objective: List the common applications that are provided by TCP/IP
  - o Topology
  - o Job Aid
  - o Task 1: Inspect TCP/IP Applications
- Challenge

Lesson 4: Exploring the Functions of Routing
Objective: Define the role, components and function of a Router Understand how a Routing Table conveys information Understand how a Router chooses a path or route Understand how Dynamic Routing protocols calculate and communicate routing information
This lesson includes these topics:

- Role of a Router
  - o Objective: Describe the role of a router in the IP packet delivery process
- Router Components
  - o Objective: Describe the physical characteristics of a router
- Router Function
  - o Objective: Describe the functions of a router
- Routing Table
  - o Objective: Describe the components of routing table
- Dynamic Routing Protocol
  - o Objective: Describe the function of dynamic routing protocols
- Path Determination
  - o Objective: Describe router path determination.
- Route Selection

- o   Objective: Describe how router selects the best path
- Challenge

Lesson 5: Configuring a Cisco Router
Objective: Implement basic configuration on a Cisco router
This lesson includes these topics:

- Initial Router Setup
    - o   Objective: Describe router startup
- Configuring Router Interfaces
    - o   Objective: Describe how to configuring router interfaces
- IP Addresses on Router Interfaces
    - o   Objective: Explain how to configure IP address on an interface and why.
- Checking Interface Configuration and Status
    - o   Objective: Explain how to check interface configuration.
- Discovery 6: Start with Cisco Router Configuration
    - o   Objective: Perform basic Cisco Router configuration
    - o   Topology
    - o   Job Aid
    - o   Task 1: Configure an IP Address on the Router Interfaces
    - o   Task 2: Verify Interface Configuration and Status
- Exploring Connected Devices
    - o   Objective: Describe the need for a network discovery protocol.
- Using Cisco Discovery Protocol
    - o   Objective: Explain how CDP operates.
- Discovery 7: Configure Cisco Discovery Protocol
    - o   Objective: Configure and verify CDP and LLDP.
    - o   Topology
    - o   Job Aid
    - o   Task 1: Discover Neighbors Using Cisco Discovery Protocol
- Configuring LLDP
    - o   Objective: Describe LLDP configuration
- Challenge
    - o   Challenge 2: Implementing the Initial Router Configuration
    - o   Objective: Learn to configure basic router settings
    - o   Topology
    - o   Job Aid

- o   Task 1: Evaluation Lab Procedure
- Command List

Lesson 6: Exploring the Packet Delivery Process
Objective: Understand host-to-host communications across switches and routers
This lesson includes these topics:

- Address Resolution Protocol
  - o   Objective: Explain the role of ARP
- Default Gateways
  - o   Objective: Elaborate what default gateway is and why it is used.
- Discovery 8: Configure Default Gateway
  - o   Objective: Describe how end systems use subnet masks and default gateways
  - o   Topology
  - o   Job Aid
  - o   Task 1: Configure Default Gateway
- Host-to-Host Packet Delivery
  - o   Objective: Describe the host-to-host packet delivery
- Role of a Switch in Packet Delivery
  - o   Objective: Describe the host-to-host packet delivery process through a switch
- Discovery 9: Exploration of Packet Forwarding
  - o   Objective: This discovery will show how packet forwarding happens through devices by observing through show commands and debugs.
  - o   Topology
  - o   Job Aid
  - o   Task 1: Exploration of Packet Forwarding
- Troubleshooting Common Problems Associated with IP Addressing
  - o   Objective: Describe the common common troubleshooting tools.
- Challenge

Lesson 7: Enabling Static Routing
Objective: Describe the operation, benefits, and limitations of static routing
This lesson includes these topics:

- Routing Operation
  - o   Objective: Describe the basic characteristics of routing operations
- Static and Dynamic Routing Comparison
  - o   Objective: Explain the differences between static and dynamic routing

- When to Use Static Routing
  - Objective: Explain when to use static routing
- Static Route Configuration
  - Objective: Describe how to configure static route configuration
- Default Routes
  - Objective: Describe how to configure default route configuration
- Verifying the Static Route Configuration
  - Objective: Describe how to verify static route configuration
- Verifying the Default Route Configuration
  - Objective: Describe how to verify default route configuration
- Discovery 10: Configure and Verify Static Routes
  - Objective: Configure static routes
  - Topology
  - Job Aid
  - Task 1: Verify Devices Reachability
  - Task 2: Configure and Verify Static Routes
  - Task 3: Demonstrate Static Route Drawback
  - Task 4: Configure and Verify the Backup Static Route
  - Task 5: Configure and Verify the Default Route
- Challenge
  - Challenge 3: Implementing Static Routing
  - Objective: Learn to configure and use static routes.
  - Topology
  - Job Aid
  - Task 1: Evaluation Lab Procedure
- Command List

Lesson 8: Learning the Basics of ACL
Objective: Describe the operation of ACLs and their applications in the network
This lesson includes these topics:

- ACL Overview
  - Objective: Describe what ACLs are
- ACL Operation
  - Objective: Explain how ACLs operate
- ACL Wildcard Masking
  - Objective: Describe ACL wildcard masking

- Wildcard Bit Mask Abbreviations
    - Objective: Describe ACL wildcard bit mask abbreviations
- Types of ACLs
    - Objective: Describe types of ACLs
- Testing an IP Packet Against a Numbered Standard Access List
    - Objective: Describe how to test an IP packet against a numbered standard access list
- Configuring Standard IPv4 ACLs
    - Objective: Explain numbered IPv4 ACLs.
- Discovery 11: Configure and Verify ACLs
    - Objective: Configure named and standard ACLs.
    - Topology
    - Job Aid
    - Task 1: Configure Numbered Standard IPv4 ACLs
    - Task 2: Filter Traffic Using ACLs
- Using ACLs to Filter Network Traffic
    - Objective: Describe traffic filtering with ACLs
- Applying ACLs to Interfaces
    - Objective: Apply an ACL to an interface
- Configuring Named ACLs
    - Objective: Configure and edit named IPv4 ACLs
- Challenge
    - Challenge 4: Implementing Basic Numbered and Named ACLs
    - Objective: Learn to configure standard and named ACLs
    - Topology
    - Job Aid
    - Task 1: Evaluation Lab Procedure
- Command List

Lesson 9: Enabling Internet Connectivity
Objective: Configure Internet access using DHCP clients, NAT, and PAT on Cisco routers
This lesson includes these topics:

- Demarcation Point
    - Objective: Explain the demarcation point
- Provider-Assigned IP Addresses
    - Objective: Expain DHCP and static addressing.

- Public vs. Private IPv4 Addresses
  - Objective:
- Discovery 12: Configure a Provider-Assigned IP Address
  - Objective: Configure a Static Provider Assigned IP address and Configuring DHCP Client
  - Topology
  - Job Aid
  - Task 1: Configure a Provider-Assigned IP Address
- Introducing NAT
  - Objective: Describe the features and benefits of NAT
- Types of Addresses in NAT
  - Objective: Describe types of NAT addresses
- Types of NAT
  - Objective: Describe types of NAT
- Understanding Static NAT
  - Objective: Explain static NAT.
- Configuring and Verifying Static NAT
  - Objective: Explain how to configure and verify static NAT.
- Discovery 13: Configure Static NAT
  - Objective: Configure static NAT and explain its operation
  - Topology
  - Job Aid
  - Task 1: Configure Static NAT
- Understanding Dynamic NAT
  - Objective: Explain dynamic NAT.
- Configuring and Verifying Dynamic NAT
  - Objective: Explain how to configure dynamic NAT.
- Understanding PAT
  - Objective: Introduce and explain PAT.
- Configuring and Verifying PAT
  - Objective: Explain how to configure and verify PAT.
- Discovery 14: Configure Dynamic NAT and PAT
  - Objective: Understand how dynamic NAT works and also to configure it
  - Topology
  - Job Aid

- o   Task 1: Configure Dynamic NAT and PAT
- Troubleshooting NAT
  - o   Objective: Illustrate how to troubleshoot NAT.
- Discovery 15: Troubleshoot NAT
  - o   Objective: Troubleshoot NAT related issues.
  - o   Topology
  - o   Job Aid
  - o   Task 1: Troubleshoot NAT
- Challenge
  - o   Challenge 5: Implementing PAT
  - o   Objective: PAT configuration and verification
  - o   Topology
  - o   Job Aid
  - o   Task 1: Evaluation Lab Procedure
- Command List

Module 3: Summary Challenge
Objective: Configure and troubleshoot topics learn in Module 1 and Module 2.

Lesson 1: Establish Internet Connectivity
Objective: Establish internet connectivity.
This lesson includes these topics:

- Challenge
  - o   Challenge 6: Summary Challenge Lab: 1
  - o   Objective: Summary Challenge lab on topics from Mod 1 and Mod 2.
  - o   Topology
  - o   Job Aid
  - o   Task 1: Evaluation Lab Procedure

Lesson 2: Troubleshoot Internet Connectivity
Objective: Troubleshoot internet connectivity.
This lesson includes these topics:

- Challenge
  - o   Challenge 7: Summary Challenge Lab: 2
  - o   Objective: Summary Challenge lab on topics from Mod 1 and Mod 2.
  - o   Topology
  - o   Job Aid

> o Task 1: Evaluation Lab Procedure

Module 4: Building a Medium-Sized Network

Objective: Expand a small network to a medium-sized network with routing enabled.

Lesson 1: Implementing VLANs and Trunks
Objective: Implement and verify VLANs and trunking
This lesson includes these topics:

- Enterprise Network Design
  - o Objective: Describe the enterprise network design.
- Issues in a Poorly Designed Network
  - o Objective: Describe the issues in poorly designed LANs
- VLAN Introduction
  - o Objective: Describe the purpose and functions of VLANs
- Creating a VLAN
  - o Objective: Explains how to create a VLAN.
- Assigning a Port to a VLAN
  - o Objective: Describes how to assign a Port to a VLAN
- Trunking with 802.1Q
  - o Objective: Define the purpose and function of trunking
- Configuring an 802.1Q Trunk
  - o Objective: Describe how to configure an 802.1Q Trunk
- Discovery 16: Configure VLAN and Trunk
  - o Objective: Configure, verify and troubleshoot VLANs and trunks.
  - o Topology
  - o Job Aid
  - o Task 1: Configure VLAN and Trunk
- VLAN Design Consideration
  - o Objective: Describe VLAN design and creation guidelines
- Physical Redundancy in a LAN
  - o Objective: Describe how redundancy in a network can cause broadcast loops and describe a solution to this problem
- Challenge
  - o Challenge 8: Troubleshooting VLANs and Trunk
  - o Objective: Configure and troubleshoot VLANs on multiple switches and configure routing of the traffic between them.
  - o Topology

- o Job Aid

- o Task 1: Evaluation Lab Procedure

- • Command List

Lesson 2: Routing Between VLANs
Objective: Describe the application and configuration of inter-VLAN routing
This lesson includes these topics:

- • Purpose of Inter-VLAN Routing

  - o Objective: Describe the need for inter-VLAN routing

- • Options for Inter-VLAN Routing

  - o Objective: Describe options for inter-VLAN routing

- • Discovery 17: Configure a Router on a Stick

  - o Objective: Configure Router on a Stick.

  - o Topology

  - o Job Aid

  - o Task 1: Configure a Router with a Trunk Link

- • Challenge

  - o Challenge 9: Implement Multiple VLANs and Basic Routing Between the VLANs

  - o Objective: Test your learning on VLANs and Inter-VLAN routing

  - o Topology

  - o Job Aid

  - o Task 1: Evaluation Lab Procedure

- • Command List

Lesson 3: Using a Cisco IOS Network Device as a DHCP Server
Objective: Configure a Cisco IOS DHCPv4 server on a Cisco router and switch
This lesson includes these topics:

- • Need for a DHCP Server

  - o Objective: Describe the need for dynamic host IP address assignment

- • Understanding DHCP

    Note This topic focuses on DHCP address allocation. Students should already be familiar with general DHCP properties and other DHCP allocation methods.

  - o Objective: Describe DHCP operation

- • Configuring a DHCP Server

  - o Objective: Configure DHCP server

- • Discovery 18: Configure a Cisco Router as a DHCP Server

- o Objective: Configure and verify Cisco routers as DHCP servers.
- o Topology
- o Job Aid
- o Task 1: Configure a Cisco Router as a DHCP Server
- Understanding DNS
  - o Objective: Describe how DNS look up works
  - o Discovery 19: Troubleshoot DHCP Issues
  - o Objective: Troubleshoot DHCP and DNS issues.
  - o Topology
  - o Job Aid
  - o Task 1: Troubleshooting DHCP Issues
- Challenge
  - o Challenge 10: Implementing a DHCP Server in on a Cisco IOS Device.
  - o Objective: Learn to configure Cisco Router as DHCP server
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure
- Command List

Lesson 4: Implementing RIPv2
Objective: Describe the operation and configuration of RIPv2.
This lesson includes these topics:

- Overview of Routing Protocols
  - o Objective: Describe the need for dynamic routing protocols
- Distance Vector and Link-State Routing Protocols
  - o Objective: Describe distance vector and link-state routing protocols
- Understanding RIPv2
  - o Objective: Describe RIPv2
- Configure RIPv2
  - o Objective: Describe how to configure RIPv2
- Verify RIPv2
  - o Objective: Describe how to verify RIPv2
- Discovery 20: Configure and Verify RIPv2
  - o Objective: Configure and verify RIPv2
  - o Topology
  - o Job Aid

- o Task 1: Configure and Verify RIPv2
- o Task 2: Adjust RIP Timers
- o Task 3: Disable RIP Auto Summary
- o Task 4: Configure a RIP Passive Interface
- o Task 5: Generate a Default RIP Route
- Discovery 21: Troubleshoot RIPv2
  - o Objective: Troubleshoot RIPv2
  - o Topology
  - o Job Aid
  - o Task 1: Troubleshoot RIPv2
- Challenge
  - o Challenge 11: Implementing RIPv2
  - o Objective: Configure and troubleshoot RIPv2.
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure
- Command List

Module 5: Network Device Management and Security
Objective: Configure, manage and monitor Cisco devices.

Lesson 1: Securing Administrative Access
Objective: Implement a basic security configuration
This lesson includes these topics:

- Network Device Security Overview
  - o Objective: List the actions that are required to secure a network device
- Securing Access to Privileged EXEC Mode
  - o Objective: Secure access to privileged EXEC mode
- Securing Console Access
  - o Objective: Secure console access to a network device
- Securing Remote Access
  - o Objective: Secure remote access to a network device
- Discovery 22: Enhance Security of Initial Configuration
  - o Objective: Learn basic configuration to secure initial config.
  - o Topology
  - o Job Aid

- - Task 1: Secure Access to Privileged EXEC Mode
  - Task 2: Secure Console and Remote Access
  - Task 3: Enable SSH
- Limiting Remote Access with ACLs
  - Objective: Limit remote access with an ACL
- Configuring the Login Banner
  - Objective: Configure the login banner
- Discovery 23: Limit Remote Access Connectivity
  - Objective: Learn how to enable and secure remote access connectivity
  - Topology
  - Job Aid
  - Task 1: Limit Remote Access with ACLs
  - Task 2: Configure the Login and EXEC Banners
- Challenge
  - Challenge 12: Securing Device Administrative Access
  - Objective: Securing access to Devices.
  - Topology
  - Job Aid
  - Task 1: Evaluation Lab Procedure
- Command List

Lesson 2: Implementing Device Hardening
Objective: Implement basic steps to harden network devices
This lesson includes these topics:

- Securing Unused Ports
  - Objective: Secure unused ports
- Port Security
  - Objective: Describe port security
- Configuring Port Security
  - Objective: Configure port security
- Verifying Port Security
  - Objective: Verify port security
- Discovery 24: Configure and Verify Port Security
  - Objective: Learn to configure Port security
  - Topology
  - Job Aid

- o Task 1: Configure and Verify Port Security
- Disabling Unused Services
  - o Objective: Disable unused services
- Network Time Protocol
  - o Objective: Describe NTP
- Configuring NTP
  - o Objective: Configure basic NTP
- Verifying NTP
  - o Objective: Verify NTP
- Discovery 25: Configure and Verify NTP
  - o Objective: Configure and verify NTP in Client Server mode.
  - o Topology
  - o Job Aid
  - o Task 1: Configure and Verify NTP
- Challenge
  - o Challenge 13: Implementing Device Hardening
  - o Objective: Learn to configure NTP and port security
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure
- Command List

Lesson 3: Configuring System Message Logging
Objective: Configure System Message Logging
This lesson includes these topics:

- Syslog Overview
  - o Objective: Explain why syslog is used
- Syslog Message Format
  - o Objective: Describe the format of syslog messages
- Syslog Configuration
  - o Objective: Configure syslog on a Cisco device
- Discovery 26: Configure Syslog
  - o Objective: Describe Syslog Configuration
  - o Topology
  - o Job Aid
  - o Task 1: Configure Syslog

- Challenge
  - Challenge 14: Configuring System Message Logging
  - Objective: Configure and verify System message logging.
  - Topology
  - Job Aid
  - Task 1: Evaluation Lab Procedure
- Command List

Lesson 4: Managing Cisco Devices
Objective: Describe the management of Cisco devices
This lesson includes these topics:

- Router Internal Components
  - Objective: Describe the major internal components of a Cisco router
- ROM Functions
  - Objective: Describe the functions of ROM in a Cisco router
- Stages of the Router Power-On Boot Sequence
  - Objective: Describe the sequence of events that occurs during a router boot
- Configuration Register
  - Objective: Describe how to display the boot information in the configuration register
- Locating Cisco IOS Image Files
  - Objective: Describe the process of locating Cisco IOS images
- Loading Cisco IOS Image Files
  - Objective: Describe the process of loading Cisco IOS images
- Loading Cisco IOS Configuration Files
  - Objective: Describe the process of loading Cisco IOS configuration files
- Cisco IOS Integrated File System and Devices
  - Objective: Describe the file systems that are used by a Cisco router
- Managing Cisco IOS Images
  - Objective: Describe why it is important to create a backup of Cisco IOS images and configuration files
- Deciphering Cisco IOS Image Filenames
  - Objective: Describe how to decipher Cisco IOS image filenames
- Managing Device Configuration Files
  - Objective: Describe the configuration files and their location
- Password Recovery

- o   Objective: Describe how to perform a password recovery on a Cisco router
- Challenge

Lesson 5: Licensing

Objective: Understand licensing under Cisco IOS 15. In this lesson we can use an EAI to demonstrate license installation and verification.

This lesson includes these topics:

- Licensing Overview
    - o   Objective: Explain Cisco IOS image licensing
- Licensing Verification
    - o   Objective: Explain how a current version of the license can be identified
- Permanent License Installation
    - o   Objective: Explain how to install a permanent license
- Evaluation License Installation
    - o   Objective: Explain how to install an evaluation license
- Backing Up the License
    - o   Objective: Explain how to back up a license
- Uninstalling the License
    - o   Objective: Explain how to uninstall a license
- Cisco Smart Software Manager
    - o   Objective: Descrive Cisco Smart Software Manager
- Challenge

Module 6: Summary Challenge

Objective: Configure and troubleshoot a medium sized network.

Lesson 1: Implementing a Medium-Sized Network
This lesson includes these topics:

- Challenge
    - o   Challenge 15: Summary Challenge Lab: 3
    - o   Objective: Based on Mod 3 and Mod 4 topics a summary challenge lab to be created.
    - o   Topology
    - o   Job Aid
    - o   Task 1: Evaluation Lab Procedure

Lesson 2: Troubleshooting a Medium-Sized Network
This lesson includes these topics:

- Challenge
    - Challenge 16: Summary Challenge Lab: 4
    - Objective: Based on Mod 3 and Mod 4 topics a summary challenge lab to be created.
    - Topology
    - Job Aid
    - Task 1: Evaluation Lab Procedure

Module 7: Introducing IPv6
Objective: Describe IPv6 basics

Lesson 1: Introducing Basic IPv6
Objective: Describe IPv6 main features, addresses.
This lesson includes these topics:

- IPv4 Addressing Exhaustion Workarounds
    - Objective: Identify issues in IPv4
- IPv6 Features
    - Objective: Identify the main IPv6 features
- IPv6 Addresses
    - Objective: Describe IPv6 addresses and address types
- IPv6 Address Scopes and Prefixes
    - Objective: Describes the IPv6 unicast addresses.
- IPv6 Address Allocation
    - Objective: Describe manual address assignment, stateless autoconfiguration, and DHCPv6
- Challenge

Lesson 2: Understanding IPv6 Operation
Objective: Describe IPv6 operations and basic IPv6 configuration.
This lesson includes these topics:

- Comparison of IPv4 and IPv6 Headers
    - Objective: Compare the IPv4 and IPv6 header
- Internet Control Message Protocol Version 6
    - Objective: Describe ICMPv6
- Neighbor Discovery
    - Objective: Describe the neighbor discovery process and mapping from IPv6 addresses to Layer 2 addresses
- Stateless Address Autoconfiguration

- o Objective: Describe and configure stateless autoconfiguration
- Discovery 27: Configure Basic IPv6 Connectivity
  - o Objective: Basic IPv6 commands
  - o Topology
  - o Job Aid
  - o Task 1: Configure IPv6 Addresses
  - o Task 2: Configure IPv6 Stateless Autoconfiguration
- Challenge

Lesson 3: Configuring IPv6 Static Routes
Objective: Identify routing protocols for IPv6
This lesson includes these topics:

- Routing for IPv6
  - o Objective: Describe routing types for IPv6
- Configuring IPv6 Static Routes
  - o Objective: Describe how to configure and verify IPv6 static routes
- Discovery 28: Configure IPv6 Static Routes
  - o Objective: Configure and verify IPv6 static routes.
  - o Topology
  - o Job Aid
  - o Task 1: Configure IPv6 Default Routes
  - o Task 2: Configure IPv6 Static Routes
- Challenge
  - o Challenge 17: Implement IPv6 Static Routing
  - o Objective: Troubleshoot IPv6 routing.
  - o Topology
  - o Job Aid
  - o Task 1: Evaluation Lab Procedure
- Command List