Certified Operating Systems Technician

COURSE INFORMATION

Course Title: Certified Operating Systems Technician

Duration: 3 Days

Language: English

Class Format Options:

Instructor-led classroom
Live Online Training

Prerequisites:

- Certified Hardware Technician Certification or Equivalent Knowledge

Student Materials:

- Student Workbook

Certification Exams:

- Certified Operating Systems Technician Exam
- Covers A+ Operating Systems Exam Objectives

CEUs: 40

WHO SHOULD ATTEND?

Anyone who is or will be working in IT

The Certified Operating Systems Technician course will kick start your career in the IT field by providing the foundational knowledge to install, configure, and support computer operating systems; this includes installing, configuring and maintaining devices, PCs, and software for end users; understanding the basics of networking and security/forensics from the operating system view; properly and safely diagnosing, resolving, and documenting common software issues; applying troubleshooting skills; providing appropriate customer support. An often-cited favorite part of the course is when we cover virtualization, security, desktop imaging, and deployment. You will also learn the security foundations needed for the various operating systems. This course maps to the mile2 Certified Operating Systems Technician exam as well as the CompTIA A+ 220-1002 certification exam.

Cybersecurity Work Force Development

C)HT™

C)OST™

C)NP™

C)SP™

All combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide*)
  *in all technical classes only
- Exam Prep Questions
- Exam

ias™ INFORMATION ASSURANCE SERVICES
pt™ PENETRATION TESTING
dr™ DISASTER RECOVERY
gs™ GENERAL SECURITY
SC™ SECURE CODING
vbp™ VIRTUALIZATION BEST PRACTICES
WS™ WIRELESS SECURITY
cf™ COMPUTER FORENSICS

mile2
CYBER SECURITY CERTIFICATIONS

ACCREDITATIONS

COMMITTEE ON NATIONAL SECURITY SYSTEMS
CNSS
SYSTEMS SECURITY FOR THE 21st CENTURY

NICCS™
NATIONAL INITIATIVE FOR
CYBERSECURITY CAREERS AND STUDIES

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

mile2

is **ACCREDITED** by the **NSA CNSS 4011-4016**
Is **MAPPED** to NIST/Homeland Security NICCS's Cyber Security Workforce Framework
is **APPROVED** on the **FBI Cyber Security Certification Requirement list (Tier 1-3)**

UPON COMPLETION

Upon completion, the **Certified Operating Systems Technician** candidate will be able to competently take the C)OST exam as well as the CompTIA A+ 220-1002 exam.

EXAM INFORMATION

The **Certified Operating Systems Technician** exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is $400 USD and must be purchased from Mile2.com.

macs
Assessment & Certification System

OUTLINE

Chapter 1 – Operating Systems
Chapter 2 – Windows Management
Chapter 3 – Network Basics
Chapter 4 – Network Protocols
Chapter 5 – Wireless Networking
Chapter 6 – Windows Networking

Chapter 7 – Virtualization and Cloud Computing
Chapter 8 – Security Principles
Chapter 9 – Security Technologies
Chapter 10 – Securing Devices and Data
Chapter 11 – SOHO Network Configurations

ias
INFORMATION ASSURANCE SERVICES

pt
PENETRATION TESTING

dr
DISASTER RECOVERY

gs
GENERAL SECURITY

SC
0010 1001 0101
SECURE CODING

vbp
VIRTUALIZATION BEST PRACTICES

WS
WIRELESS SECURITY

cf
COMPUTER FORENSICS

DETAILED OUTLINE

Chapter 1: Operating Systems

Section 1: Windows versions and features

Section 2: Windows installation and upgrades

Section 3: Non-Windows operating systems

Section 4: Applications and Scripting

Chapter 2: Windows Management

Section 1: Operating system features and tools

Section 2: Control Panel utilities

Section 3: Command-line tools

Section 4: Troubleshooting

Chapter 3: Network Basics

Section 1: Classifying Networks

Section 2: Network Devices

Section 3: Internet Connections

Chapter 4: Network Protocols

Section 1: TCP/IP Settings

Section 2: Transport Protocols

Section 3: Application Protocols

Chapter 5: Wireless Networking

Section 1: Wi-Fi Standards

Section 2: Wireless Encryption

Chapter 6: Windows Networking

Section 1: Sharing and Security

Section 2: Network Connections

Section 3: Connection Troubleshooting

Chapter 7: Virtualization and Cloud Computing

Section 1: Virtualization

Section 2: Cloud Computing

Chapter 8: Security Principles

Section 1: Threats and Vulnerabilities

Section 2: Security Controls

Chapter 9: Security Technologies

Section 1 – Operating System Securities

Section 2 – Security Hardware and Software

Chapter 10: Securing Devices and Data

Section 1 – Workstation Security

Section 2 – Mobile Device Security

Section 3 – Security Troubleshooting

Chapter 11: SOHO Network Configurations

Section 1 – SOHO Router Features

Section 2 – Network Security