IT-2740: FUNDAMENTALS OF CLIENT OPERATING SYSTEMS AND HARDWARE FOR CYBERSECURITY

Cuyahoga Community College

Viewing: IT-2740 : Fundamentals of Client Operating Systems and Hardware for Cybersecurity

Academic Term:

Fall 2021

Subject Code

IT - Information Technology

Course Number:

2740

Title:

Fundamentals of Client Operating Systems and Hardware for Cybersecurity

Catalog Description:

Provides an introduction to and basic technical understanding of the function and operation of operating systems and computing hardware with consideration given to relevant security best practices.

Credit Hour(s):

4

Lecture Hour(s):

3

Lab Hour(s):

2

Requisites

Prerequisite and Corequisite

IT-1025 Information Technology Concepts for Programmers.

Outcomes

Course Outcome(s):

Apply fundamental concepts of operating systems, file systems, networking, security, backup and recovery procedures to troubleshoot, maintain and support secure client operating systems and hardware.

Objective(s):

1. Explain the basic components of a microcomputer.
2. Demonstrate methods for securing the desktop in a small office/home office (SOHO) wireless and wired networks.
3. Identify common symptoms and problems associated with each subsystem and how to troubleshoot and isolate the problem.
4. Compare and contrast the features and requirements of common operating systems including installation and secure configuration.
5. Explain the boot-up sequences of common operating systems.
6. Compare and contrast common client operating system file systems.
7. Mitigate common operating system security threats and vulnerabilities, and best practices to secure a workstation.
8. Explain the major components of a printer.
9. Explain the basic features of mobile operating systems and compare and contrast methods for securing mobile devices.
10. Discuss appropriate methods of securing data, data recovery, and data destruction and disposal methods.
11. Explain application installation and configuration concepts.
12. Discuss best practices associated with operational procedures.
13. Explain virtualization and cloud computing.

Methods of Evaluation:

Evaluation can include any combination of the following:

1. Assignments
2. Quizzes
3. Exams
4. Lab Assignments
5. Projects
6. Reports
7. Oral Evaluations

Course Content Outline:

1. Hardware Concepts for Securing Desktop Environments
   a. Configure and use BIOS/UEFI tools settings on a PC
   b. Motherboard components, identification, their purpose and properties
   c. Current common RAM types and their features and compatibility
   d. Current commonly used storage devices and media
   e. Various current common types of CPUs, their characteristics, and appropriate cooling methods
   f. Common current PC connection interfaces, their characteristics and purpose
   g. Types of current common display devices and their features (examples)
   h. Common PC connector types and their associated cables
   i. Basic hardware troubleshooting concepts
   j. Common peripheral devices
2. Mobile Device Concepts for Cybersecurity
   a. Common laptop hardware components and their function
   b. Other mobile device types and their characteristics
3. Operating Systems Concepts for Securing Desktop and Mobile Environments
   a. Features and requirements of current common Microsoft operating systems, including upgrade paths
   b. Windows PC operating systems installation methods and configurations
   c. Microsoft command line tools and their applications
   d. Use of appropriate Microsoft operating system features, utilities and tools
   e. Use of Windows Control Panel utilities
   f. Windows Networking Configuration on a client/desktop; alternatives and settings
   g. Common preventive maintenance procedures and best practices using the appropriate Windows OS tools
   h. Common features and functionality of the Mac OS and Linux operating systems:
   i. Best practices for maintaining and securing Mac OS and Linux OS and their tools
   j. Basic Linux commands
   k. Mobile operating systems basic features Android vs. iOS vs. Windows
   l. Common security threats and vulnerabilities
   m. Common prevention methods for security
   n. Basic Windows OS security settings
   o. Best practices to secure a workstation
   p. Methods for securing mobile devices
   q. Appropriate data and media destruction and disposal methods
   r. Securing operating systems in SOHO wireless and wired networks
   s. Software application installation requirements, methods and security
4. Troubleshooting Concepts for Securing Desktop Environments:
   a. Basic troubleshooting concepts
   b. Troubleshooting PC common operating system problems with appropriate tools
   c. Troubleshooting common PC security issues with appropriate tools and best practices and procedures
   d. Troubleshooting common mobile OS and application security issues with appropriate tools
   e. Troubleshooting theory and best practices
5. Operational Procedures
   a. Documentation types
   b. Change management
   c. Safety procedures
   d. Disaster prevention and recovery
   e. Potential environmental impacts on equipment and devices, and the appropriate controls
   f. Address prohibited content/activity, and explain privacy, licensing and policy concepts

    g. Proper communication techniques and professionalism
6. Virtualization and Cloud Computing Concepts
    a. Common cloud models
    b. Purpose of virtual machines
    c. Resource requirements
    d. Security requirements

Resources

Jean Andrews. *CompTIA A+ Guide to IT Technical Support* . 10th. Cengage, 2020.

Jean Andrews. *Guide to Operating Systems and Security*. 10th. Cengage, 2020.

Jean Andrews. *Guide to Computing Infrastructure*. 10th. Cengage, 2020.

Brian Knittel, Paul McFedries. *Windows 10 In Depth*. 2nd . Pearson / Que, 2018.

Scott Mueller. *Upgrading and Repairing PCs.* 22nd. Que, 2015.

Mike Meyers. *CompTIA A+ Certification All-in-One Exam Guide*. 10th. McGraw-Hill Education, 2019.

Top of page

Key: 2517