A+ (220-1102)

Project Workbook
Student Edition

Presented By
LearnKey®

A+ (220-1102) Project Workbook

First Edition

LearnKey creates signature multimedia courseware. LearnKey provides expert instruction for popular computer software, technical certifications, and application development with dynamic video-based courseware and effective learning management systems. For a complete list of courses, visit https://www.learnkey.com.

LearnKey

Table of Contents

Introduction

A+ (220-1102)

LearnKey

Best Practices Using LearnKey's Online Training

LearnKey offers video-based training solutions that are flexible enough to accommodate private students and educational facilities and organizations.

Our course content is presented by top experts in their respective fields and provides clear and comprehensive information. The full line of LearnKey products has been extensively reviewed to meet superior quality standards. Our course content has also been endorsed by organizations such as Certiport, CompTIA®, Cisco, and Microsoft. However, it is the testimonials given by countless satisfied customers that truly set us apart as leaders in the information training world.

LearnKey experts are highly qualified professionals who offer years of job and project experience in their subjects. Each expert has been certified at the highest level available for their field of expertise. This expertise provides the student with the knowledge necessary to obtain top-level certifications in their chosen field.

Our accomplished instructors have a rich understanding of the content they present. Effective teaching encompasses presenting the basic principles of a subject and understanding and appreciating organization, real-world application, and links to other related disciplines. Each instructor represents the collective wisdom of their field and within our industry.

Our Instructional Technology

Each course is independently created based on the manufacturer's standard objectives for which the course was developed.

We ensure that the subject matter is up-to-date and relevant. We examine the needs of each student and create training that is both interesting and effective. LearnKey training provides auditory, visual, and kinesthetic learning materials to fit diverse learning styles.

Course Training Model

The course training model allows students to undergo basic training, building upon primary knowledge and concepts to more advanced application and implementation. In this method, students will use the following toolset:

Pre-assessment: The pre-assessment is used to determine the student's prior knowledge of the subject matter. It will also identify a student's strengths and weaknesses, allowing them to focus on the specific subject matter they need to improve the most. Students should not necessarily expect a passing score on the pre-assessment as it is a test of prior knowledge.

Video training sessions: Each training course is divided into sessions or domains and lessons with topics and subtopics. LearnKey recommends incorporating all available external resources into your training, such as student workbooks, glossaries, course support files, and additional customized instructional material. These resources are located in the folder icon at the top of the page.

Exercise labs: Labs are interactive activities that simulate situations presented in the training videos. Step-by-step instructions and live demonstrations are provided.

Post-assessment: The post-assessment is used to determine the student's knowledge gained from interacting with the training. In taking the post-assessment, students should not consult the training or any other materials. A passing score is 80 percent or higher. If the individual does not pass the post-assessment the first time, LearnKey recommends incorporating external resources, such as the workbook and additional customized instructional material.

Workbook: The workbook has various activities, including fill-in-the-blank questions, short answer questions, practice exam questions, and group and individual projects that allow the student to study and apply concepts presented in the course videos.

Using This Workbook

This project workbook contains practice projects and exercises to reinforce the knowledge you have gained through the video portion of the **A+ (220-1102)** course. The purpose of this workbook is twofold. First, get you further prepared to pass the [exam name] exam, and second, to teach you job-ready skills and increase your employability in the area of [body of knowledge].

The projects within this workbook follow the order of the video portion of this course. To save your answers in this workbook, you must first download a copy to your computer. You will not be able to save your answers in the web version. You can complete the workbook exercises as you go through each section of the course, complete several at the end of each domain, or complete them after viewing the entire course. The key is to go through these projects to strengthen your knowledge in this subject.

Each project is based upon a specific video (or videos) in the course and specific test objectives. The materials you will need for this course include:

- LearnKey's **A+ (220-1102)** courseware.
- The course project files. All applicable project files are located in the support area where you downloaded this workbook.
- A laptop
- Installation media for Windows 10 Professional and an edition of Linux
- Access to a Mac
- Access to a printer for configuration purposes
- Access to a shared folder on another device
- Access to a smartphone or tablet

For Teachers

LearnKey is proud to provide extra support to instructors upon request. For your benefit as an instructor, we also provide an instructor support .zip file containing answer keys, completed versions of the workbook project files, and other teacher resources. This .zip file is available within your learning platform's admin portal.

Notes

- Extra teacher notes, when applicable, are in the Project Details box within each exercise.
- Exam objectives are aligned with the course objectives listed in each project, and project file names correspond with these numbers.
- The Finished folder in each domain has reference versions of each project. These can help you grade projects.
- Short answers may vary but should be similar to those provided in this workbook.
- Teachers may consider asking students to add their initials, student ID, or other personal identifiers at the end of each saved project.
- Refer to your course representatives for further support.

We value your feedback about our courses. If you have any questions, comments, or concerns, please let us know by visiting https://about.learnkey.com.

Skills Assessment

Instructions: Rate your skills on the following tasks from 1-5 (1 being needs improvement, 5 being excellent).

Skills	1	2	3	4	5
Identify basic features of Microsoft Windows editions.	□	□	□	□	□
Given a scenario, use the appropriate Microsoft command-line tool.	□	□	□	□	□
Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).	□	□	□	□	□
Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.	□	□	□	□	□
Given a scenario, use the appropriate Windows settings.	□	□	□	□	□
Given a scenario, configure Microsoft Windows networking features on a client/desktop.	□	□	□	□	□
Given a scenario, apply application installation and configuration concepts.	□	□	□	□	□
Explain common OS types and their purposes.	□	□	□	□	□
Given a scenario, perform OS installations and upgrades in a diverse OS environment.	□	□	□	□	□
Identify common features and tools of the macOS/desktop OS.	□	□	□	□	□
Identify common features and tools of the Linux client/desktop OS.	□	□	□	□	□
Summarize various security measures and their purposes.	□	□	□	□	□
Compare and contrast wireless security protocols and authentication methods.	□	□	□	□	□
Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.	□	□	□	□	□
Explain common social engineering attacks, threats, and vulnerabilities.	□	□	□	□	□
Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.	□	□	□	□	□
Given a scenario, configure a workstation to meet best practices for security.	□	□	□	□	□
Explain common methods for securing mobile and embedded devices.	□	□	□	□	□
Given a scenario, use common data destruction and disposal methods.	□	□	□	□	□
Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.	□	□	□	□	□

Skills	1	2	3	4	5
Given a scenario, install and configure browsers and relevant security settings.	□	□	□	□	□
Given a scenario, troubleshoot common Windows OS problems.	□	□	□	□	□
Given a scenario, troubleshoot common personal computer (PC) security issues.	□	□	□	□	□
Given a scenario, use best practice procedures for malware removal.	□	□	□	□	□
Given a scenario, troubleshoot common mobile OS and application issues.	□	□	□	□	□
Given a scenario, troubleshoot common mobile OS and application security issues.	□	□	□	□	□
Given a scenario, implement best practices associated with documentation and support systems information management.	□	□	□	□	□
Explain basic change-management best practices.	□	□	□	□	□
Given a scenario, implement workstation backup and recovery methods.	□	□	□	□	□
Given a scenario, use common safety procedures.	□	□	□	□	□
Summarize environmental impacts and local environmental controls.	□	□	□	□	□
Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.	□	□	□	□	□
Given a scenario, use proper communication techniques and professionalism.	□	□	□	□	□
Identify the basics of scripting.	□	□	□	□	□
Given a scenario, use remote access technologies.	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□

A+ (220-1102) Video Times

Domain 1	Video Time
Windows Features	00:15:44
Command Line Tools	00:30:25
Windows 10 Features and Tools	00:26:28
Control Panel Utilities	00:28:12
Windows Settings	00:13:49
Client Networking Features	00:23:31
App Installs and Configurations	00:12:16
OS Types and Their Purposes	00:13:47
OS Installations	00:18:45
macOS Tools and Features	00:26:56
Linux Tools and Features	00:26:53
Total Time	**03:56:46**

Domain 2	Video Time
Security Measures	00:35:00
Wireless Security Protocols	00:07:13
Malware	00:16:02
Social Engineering	00:21:38
Windows Security Settings	00:23:38
Workstation Best Practices	00:17:42
Securing Mobile Devices	00:15:52
Data Destruction and Disposal	00:06:28
SOHO Network Security Settings	00:21:39
Install and Configure Browsers	00:12:12
Total Time	**02:57:24**

Domain 3	Video Time
Common Windows OS Problems	00:36:14
Common PC Security Issues	00:12:06
Malware Removal Best Practices	00:09:41
Common Mobile OS and App Issues	00:12:56
Common Mobile OS and App Security Issues	00:17:29
Total Time	**01:28:26**

Domain 4	Video Time
Documentation Best Practices	00:22:45
Change Management Best Practices	00:09:04
Backup and Recovery	00:08:49
Common Safety Procedures	00:10:19
Environmental Impacts and Controls	00:07:45
Content, Licensing, and Policies	00:12:50
Communication and Professionalism	00:13:52
Scripting Basics	00:18:31
Remote Access Technologies	00:12:37
Total Time	**01:56:32**

Domain 1:
Lesson 1

A+ (220-1102)

Windows 10 Editions

Windows 10, a very popular operating system for desktop and laptop computers, comes in many different editions. Each edition has its own set of features and limitations as to what it can support physically, especially in the area of RAM.

Technicians need to use this information to match people with the most cost-effective edition of Windows for their use while ensuring the edition of Windows covers people's needs adequately.

Purpose

Upon completing this project, you will better understand Windows 10 editions, their features, and their limitations.

Steps for Completion

1. Which edition of Windows 10 supports volume licensing?

   a. ____

2. What is the maximum amount of RAM for each edition of Windows 10?

   a. Home: ____________________________________

   b. Pro: ______________________________________

   c. Pro for Workstations: ______________________

3. List at least two features Windows 10 Pro has that Windows 10 Home does not support:

   a. ____

   ____

4. Which version of Windows do you have?

   a. ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: Windows Features

Subtopic: Windows 10 Editions

Objectives covered

1 Operating Systems

1.1 Identify basic features of Microsoft Windows editions

1.1.1 Windows 10 editions

1.1.1.1 Home

1.1.1.2 Pro

1.1.1.3 Pro for Workstations

1.1.1.4 Enterprise

Windows Feature Differences

Part of deciding which edition of Windows to install on a device involves knowing the features available, especially the features the Pro edition has versus the Home edition. For example, Windows Home cannot join a domain. Only Windows Pro or higher can join a domain.

Purpose

Upon completing this project, you will better understand the feature differences among Windows editions.

Steps for Completion

1. On a Windows 10 device, access your advanced system settings.
2. Is your computer inside a workgroup or domain?
   a. ______________________________
   ____
3. Can your device host Remote Desktop Connections?
   a. ______________________________
   ____
4. What is the maximum amount of RAM a 32-bit edition of Windows can support?
   a. ______________________________
5. Can you open BitLocker or Group Policy Editor on your device?
   a. ______________________________
   ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1
Topic: Windows Features
Subtopics: Domains vs. Workgroups; Desktop Styles and RDP; RAM Support Limitations; BitLocker; Gpedit

Objectives covered

1 Operating Systems
1.1 Identify basic features of Microsoft Windows editions
1.1.2 Feature differences
1.1.2.1 Domain access vs. workgroup
1.1.2.2 Desktop styles/user interface
1.1.2.3 Availability of Remote Desktop Protocol (RDP)
1.1.2.4 Random-access memory (RAM) support limitations
1.1.2.5 BitLocker
1.1.2.6 Gpedit.msc

Upgrade Paths

As operating systems become obsolete and new versions of an operating system are released, people will want to upgrade to the newer one. One such type of upgrade is an in-place upgrade, in which a person's files, folders, and settings are kept intact. Technicians need to know the viable paths for upgrading from one operating system to another and upgrading editions within an operating system.

Purpose

Upon completing this project, you will better understand upgrade paths to Windows 10.

Steps for Completion

1. On a web browser, search for and access the Microsoft document containing the upgrade paths to Windows 10.
2. To which versions can Windows 10 Home upgrade?
   a. ______________________________
3. To which versions can Windows 10 Pro upgrade?
   a. ______________________________
4. Which older editions of Windows 10 can upgrade to Windows 10?
   a. ______________________________
5. Describe what someone with Windows 8 needs to do to upgrade to Windows 10.
   a. ______________________________
   ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1
Topic: Windows Features
Subtopic: Upgrade Paths

Objectives covered

1 Operating Systems
1.1 Identify basic features of Microsoft Windows editions
1.1.3 Upgrade paths
1.1.3.1 In-place upgrade

Domain 1:

Lesson 2

A+ (220-1102)

Navigation Commands

Though most Windows settings can be changed through a graphical user interface, a command prompt is still valuable as many commands can be added to scripts and run as a group. For example, if an app or process requires a folder to be created, a script can create the folder and eliminate the need for a person to add the folder manually.

Purpose

Upon completing this project, you will better understand navigation commands and how they are used in a command-line setting.

Steps for Completion

1. On a Windows device, open a command prompt.
2. Navigate to the C:\Users\username\Documents folder to where username is your username on your device.
3. List the contents of your Documents folder. How many subdirectories are in your Documents folder?
   a. ______________________________
4. Within your Documents folder, create two directories: **test1** and **test2**
5. Delete the **test2** directory you just created.
6. What drive letters can you navigate to besides drive C: on your device?
   a. ______________________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1
Topic: Command Line Tools
Subtopics: Cd; Dir; Md; Rmdir; Drive Navigation

Objectives covered

1 Operating Systems
1.2 Given a scenario, use the appropriate Microsoft command-line tool
1.2.1 Navigation
1.2.1.1 cd
1.2.1.2 dir
1.2.1.3 md
1.2.1.4 rmdir
1.2.1.5 Drive navigation inputs:
1.2.1.5.1 C: or D: or X:

Command Line Tools – Part 1

Though most computer administrative tasks can be done using graphical user interfaces (GUIs), many tasks can be done in a command window using command line tools. The benefit of these tools is twofold: first, most require minimal typing, and, secondly, most commands can be used in scripts, which help automate processes.

Purpose

Upon completing this project and the following two projects, you will better understand command line tools and their uses.

Steps for Completion

1. On a Windows device, open a command prompt.
2. Run the command necessary to get the IP address of your device and write the address here:
    a. ______________________________
3. Ping the comptia.org domain. How many responses do you get?
    a. ______________________________
    ____
4. What is the hostname of your device?
    a. ______________________________
5. Use the help with the netstat command to answer this question: How does one run netstat to display all connections and listening ports?
    a. ______________________________
6. Use the command necessary to get the IPv4 address of the DNS server for google.com. What is that address?
    a. ______________________________
7. A person tries to run the chkdsk command and is denied access to the command. Why?
    a. ______________________________

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 1

Topic: Command Line Tools

Subtopics: Ipconfig and Help; Ping; Hostname; Netstat; Nslookup; Chkdsk

Objectives covered

1 Operating Systems

1.2 Given a scenario, use the appropriate Microsoft command-line tool

1.2.2 Command-line tools

1.2.2.1 ipconfig

1.2.2.2 ping

1.2.2.3 hostname

1.2.2.4 netstat

1.2.2.5 nslookup

1.2.2.6 chkdsk

1.2.2.18 [command name] /?

Domain 1:
Lesson 3

A+ (220-1102)

Command Line Tools – Part 2

Part of learning command line tools is knowing the differences between similarly named tools. For example, as you will see in this project, three different command line tools copy files, each with a specific purpose for copying files and folders.

Purpose

Upon completing this project, you will better understand command line tools that copy files and folders.

Steps for Completion

1. On a Windows device, open a command prompt.
2. Run the net user command, along with your username. When was your password last set?
   a. ______________________________
3. Trace the route from your device to comptia.org. How many hops are in the route?
   a. ______________________________
   ____
4. Navigate to your student folder using the commands you have learned in this course.
5. Use the copy command to copy the **scriptstart1.txt** file from the **1101** folder to the **1102** folder.
6. Use the xcopy command to copy the contents, including the subdirectories, of the **1103** folder into the **1104** folder.
7. Use the robocopy command to copy all the contents from the **1105** folder to the **1106** folder.
8. What would the command be to map the X: drive to a folder named testfiles on a server named testserver1?
   a. ______________________________
9. A person wants to erase the data on a drive E on a device. What is the command for this task?
   a. ______________________________

Project Details

Project file

Folders 1101, 1102, 1103, 1104, 1105, and 1106

Estimated completion time

10 minutes

Video reference

Domain 1
Topic: Command Line Tools
Subtopics: Net user; Net use; Tracert; Format; Xcopy and copy; Robocopy

Objectives covered

1 Operating Systems
1.2 Given a scenario, use the appropriate Microsoft command-line tool
1.2.2 Command-line tools
1.2.2.7 net user
1.2.2.8 net use
1.2.2.9 tracert
1.2.2.10 format
1.2.2.11 xcopy
1.2.2.12 copy
1.2.2.13 robocopy

Command Line Tools – Part 3

This project is the third of three projects focusing on command line tools. As a reminder, one of the main benefits of knowing these tools is to use these tools in scripts to automate processes. For example, if an app installation requires a restart, a script with the installation and the shutdown command can be built to help automate the installation.

Purpose

After completing this and the previous two projects, you will better understand command line tools and their uses on devices.

Steps for Completion

1. On a Windows device, open a command prompt.
2. Run the command that will update the Group Policy on the device.
3. Run the command that shows a resultant set of the Group Policies applied to both the user and computer on your current device. How many security groups is the user a part of?
    a. ______________________________
4. Use the diskpart command to see the list of disks on your device. How many disks are present?
    a. ______________________________
5. Run a pathping to google.com. How many hops are on the path?
    a. ______________________________
6. Run the command that displays the version of Windows on your device and then record that version here:
    a. ______________________________
7. Which attribute on the sfc command scans for and, if necessary, repairs system files?
    a. ______________________________
8. What is the command used to shut down and restart a device?
    a. ______________________________

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 1
Topic: Command Line Tools
Subtopics: Gpupdate and Gpresult; Shutdown; Sfc; Diskpart; Pathping; Winver

Objectives covered
1 Operating Systems
1.2 Given a scenario, use the appropriate Microsoft command-line tool
1.2.2 Command-line tools
1.2.2.14 gpupdate
1.2.2.15 gpresult
1.2.2.16 shutdown
1.2.2.17 Sfc
1.2.2.19 diskpart
1.2.2.20 pathping
1.2.2.21 Winver

Domain 1:

Lesson 4

A+ (220-1102)

Task Manager

Task Manager is a tool technicians use when a device is experiencing sluggish performance, as Task Manager has tools that can help pinpoint the cause of a device's performance issues. Task Manager also allows technicians to stop processes causing problems, such as a process that continues to run after its app has closed, thus using RAM unnecessarily.

Purpose

Upon completing this project, you will better understand Task Manager and its role in managing a device.

Steps for Completion

1. On a Windows device, open Task Manager.
2. Within Task Manager, restart the Spooler service.
3. Navigate to the Processes tab.
4. Which process is using the most memory?
    a. ______________________________
5. Navigate to the Startup tab.
6. How many apps/processes have their startup status set to enabled?
    a. ______________________________
7. Navigate to the Performance tab.
8. What is the current CPU utilization percentage?
    a. ______________________________
9. Navigate to the Users tab.
10. How many users are signed in to the device?
    a. ______________________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: Windows 10 Features and Tools

Subtopics: Services; Startup; Performance; Processes and Users

Objectives covered

1 Operating Systems

1.3 Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS)

1.3.1 Task Manager

1.3.1.1 Services

1.3.1.2 Startup

1.3.1.3 Performance

1.3.1.4 Processes

1.3.1.5 Users

LearnKey

Microsoft Management Console – Part 1

The Microsoft Management Console (MMC) is a tool that allows technicians to add tools, primarily administrative tools, to one console window. MMC provides a means by which one can quickly perform administrative and similar tasks on a local device and, in many cases, other devices.

Purpose

Upon completing this project, you will better understand how the MMC provides a means by which technicians can perform administrative tasks on a device.

Steps for Completion

1. On a Windows device, open the Microsoft Management Console.
2. Add the following snap-ins, setting each to view information on the local device:
   a. Event Viewer
   b. Disk Management
   c. Task Scheduler
   d. Device Manager
   e. Certificate Manager
3. Save the console as **Console1.msc** to your Student folder.
4. Access the Event Viewer. How many error messages have appeared in the last seven days?
   a. ______________________________
5. Within Disk Management, rescan disks to see if any new disks appear.
6. Within the Task Scheduler, display all running tasks. How many tasks are currently running?
   a. ______________________________
7. Access Device Manager. Are any devices shown not to be working?
   a. ______________________________
8. Access the Personal Certificates area under Certificate Manager. How many personal certificates are displayed?
   a. ______________________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: Windows 10 Features and Tools

Subtopics: Event Viewer; Disk Management; Task Scheduler; Device Manager; Certificate Manager

Objectives covered

1 Operating Systems

1.3 Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS)

1.3.2 Microsoft Management Console (MMC) snap-in

1.3.2.1 Event Viewer (eventvwr.msc)

1.3.2.2 Disk Management (diskmgmt.msc)

1.3.2.3 Task Scheduler (taskschd.msc)

1.3.2.4 Device Manager (devmgmt.msc)

1.3.2.5 Certificate Manager (certmgr.msc)

Domain 1:

Lesson 5

A+ (220-1102)

Microsoft Management Console – Part 2

This project is the second of two projects covering tools people can add to the Microsoft Management Console. The key point to know for the exam is that the MMC is used as a customizable, central point for technicians to perform administrative and similar tasks on local and, in many cases, other people's devices.

Purpose

Upon completing the previous project and this project, you will better understand MMC's role in helping technicians perform administrative tasks on devices.

Steps for Completion

1. On a Windows device, open the Microsoft Management Console.
2. Add the following snap-ins to the console, making sure each snap-in points to the local device:
   a. Local Users and Groups
   b. Performance Monitor
   c. Group Policy Editor (if available)
3. Within Local Users and Groups, how many user accounts are on the device?
   a. ______________________________
4. What is currently being tracked using Performance Monitor?
   a. ______________________________
5. Under Group Policy Editor, what are the categories of configurations?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Windows 10 Features and Tools
Subtopics: Local Users and Groups; Performance Monitor; Group Policy Editor

Objectives covered
1 Operating Systems
1.3 Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS)
1.3.2 Microsoft Management Console (MMC) snap-in
1.3.2.6 Local Users and Groups (lusrmgr.msc)
1.3.2.7 Performance Monitor (perfmon.msc)
1.3.2.8 Group Policy Editor (gpedit.msc)

LearnKey

Additional Tools

Outside of MMC, there are additional tools technicians can use to configure, support, and improve the overall performance and experience on a Windows device. Some tools help define a device’s expectations, while others focus on improvement, especially in the case of disk performance.

Purpose

Upon completing this project, you will better understand some of the tools available to configure, support, and improve Windows performance on a device.

Steps for Completion

1. Open the System Information tool on a Windows device. How much RAM is present on your device?
   a. ______________________________
2. Open the Resource Monitor tool. What is the current CPU percentage being used on your device?
   a. ______________________________
3. Open the Disk Cleanup tool.
4. Set the Disk Cleanup tool to clean drive C. How much disk space will cleaning drive C recover?
   a. ______________________________
5. Which type of hard drive benefits most from running the Optimize Drives tool?
   a. ______________________________
6. Which tool is used to set a system to boot into Safe Mode the next time the system is booted up?
   a. ______________________________
7. How many hives are used to store entries in a system registry?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 1
Topic: Windows 10 Features and Tools
Subtopics: System Information; Resource Monitor; System Configuration; Disk Cleanup; Disk Defragment; Registry Editor

Objectives covered
1 Operating Systems
1.3 Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS)
1.3.3 Additional tools
1.3.3.1 System Information (msinfo32.exe)
1.3.3.2 Resource Monitor (resmon.exe)
1.3.3.3 System Configuration (msconfig.exe)
1.3.3.4 Disk Cleanup (cleanmgr.exe)
1.3.3.5 Disk Defragment (dfrgui.exe)
1.3.3.6 Registry Editor (regedit.exe)

Domain 1:

Lesson 6

A+ (220-1102)

Control Panel Utilities – Part 1

Though the Control Panel is being phased out in usage for the Settings feature in Windows with each new edition of Windows, the Control Panel still has many applets that serve as configuration features for Windows devices.

Furthermore, the core of the Control Panel and most of its applets have not changed drastically over several editions of Windows, meaning that people familiar with the Control Panel in Windows 7 will not see much change for Windows 10.

Purpose

Upon completing this and the other Control Panel projects, you will better understand Control Panel features and their uses.

Steps for Completion

1. On a Windows device, open the Control Panel.
2. Open the Devices and Printers area. For your default printer, are any print jobs in the queue?
   a. ____________________
3. Open the Programs and Features applet.
4. Enable the Network File Services feature on your device.
5. Open the Network and Sharing Center applet. How many active connections do you have on your device?
   a. ____________________
6. Open the System utility. How much RAM is installed on the device?
   a. ____________________
7. Through the System utility, ensure system failures are being written to the system log.
8. The Control Panel applet Internet Options controls specific settings for which internet browser?
   a. ____________________
9. Close any open Control Panel utilities.

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: Control Panel Utilities

Subtopics: Internet Options; Devices and Printers; Programs and Features; Network and Sharing Center; System

Objectives covered

1 Operating Systems

1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility

1.4.1 Internet Options

1.4.2 Devices and Printers

1.4.3 Programs and Features

1.4.4 Network and Sharing Center

1.4.5 System

LearnKey

Control Panel Utilities – Part 2

This project is the second project in a series of Control Panel projects. Very few Control Panel applets do not have an equivalent area in Settings. Still, people who have been using Windows for several years may like the familiarity of the Control Panel and its utilities.

Purpose

After completing this project, you will better understand some Control Panel utilities and their role in configuring Windows.

Steps for Completion

1. On a Windows device, open the Control Panel.
2. Ensure that Windows Defender Firewall is on.
3. The Mail applet is used to configure profiles for which app?
   a. ______________________________
4. Open the Sound applet.
5. Test your speakers to make sure they are outputting sound.
6. Open the User Accounts applet. How many user accounts are on your device?
   a. ______________________________
7. Open the Device Manager applet and indicate the number of devices that are in the following modes:
   a. Devices with warning labels: ____________________
   b. Devices that are not working: ____________________
   c. Devices that are disabled: ____________________
8. Close any open Control Panel utilities.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Control Panel Utilities
Subtopics: Windows Defender Firewall; Mail; Sound; User Accounts; Device Manager

Objectives covered
1 Operating Systems
1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility
1.4.6 Windows Defender Firewall
1.4.7 Mail
1.4.8 Sound
1.4.9 User Accounts
1.4.10 Device Manager

Domain 1:

Lesson 7

A+ (220-1102)

Indexing and Administrative Tools

Indexing is a feature that speeds up searches on selected folders on a device. Indexing adds overhead to a device's performance when indexed folders are being updated, so indexing is best used on folders that have files accessed often.

Administrative tools show information on a device and offer configuration options for a device. Technicians should have at least a cursory idea of the shortcuts to tools available via the Administrative Tools applet.

Purpose

Upon completing this project, you will better understand the roles of indexing and administrative tools.

Steps for Completion

1. On a Windows 10 device, open the Control Panel.
2. Open the Indexing Options applet.
3. Ensure that Internet Explorer History is not being indexed.
4. Open the Administrative Tools applet.
5. Which ODBC Data Sources applets are available?
   a. ______________________________
6. Which two monitoring apps are available through Administrative Tools?
   a. ______________________________
7. Close the Indexing Options and Administrative Tools applets.

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: Control Panel Utilities

Subtopics: Indexing Options; Administrative Tools

Objectives covered

1 Operating Systems

1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility

1.4.11 Indexing Options

1.4.12 Administrative Tools

File Explorer Options

File Explorer is the applet showing the location of all drives, folders, and files on a device. Utilities such as the Control Panel can also be accessed through File Explorer. File Explorer can be configured to show fewer files for those who want simplicity in working with files and folders or show more files and file extensions for those who do more of their configurations on devices.

Purpose

You will better understand File Explorer options and settings after completing this project.

Steps for Completion

1. On a Windows device, open File Explorer.
2. Navigate to your user account folder under C:\Users.
3. Show the hidden files on your device. What folder appears when hidden files are shown?
   a. ______________________________
4. Hide the file extensions for files within Explorer.
5. Open the Folder Options dialog box.
6. Restore the defaults on the General tab.
7. Navigate to the View tab.
8. Enable the Don’t show hidden files, folders, or drives options.
9. Change the setting that hides extensions for known file types so that they are not hidden.
10. Close the Folder Options dialog box.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Control Panel Utilities
Subtopics: Show Hidden Files; Hide Extensions; General and View Options

Objectives covered
1 Operating Systems
1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility
1.4.13 File Explorer options
1.4.13.1 Show hidden files
1.4.13.2 Hide extensions
1.4.13.3 General options
1.4.13.4 View options

LearnKey

Power Options

Devices have power options, specifically as they relate to displays and, for laptops, what happens when a laptop's lid is closed. Different sleep modes affect the RAM on a device and what one can expect when opening the lid back up on a laptop or turning a display back on.

Purpose

Upon completing this project, you will better understand power options and their uses on a device. NOTE: You will need a laptop to complete this exercise in its entirety.

Steps for Completion

1. On a Windows device, open the Control Panel.
2. Open Power Options. Which power plan are you currently using?
   a. ______________________________
3. Access the Choose when to turn off the display option. What is your setting for turning off the display?
   a. ______________________________
4. In which sleep state is a snapshot of RAM taken?
   a. ______________________________
5. In which sleep state is there no RAM transfer off the hard drive?
   a. ______________________________
6. In which sleep state does only the display go to sleep?
   a. ______________________________
7. If you have a laptop, access the Choose what closing the lid does settings. What setting do you have for closing the lid when the laptop is plugged in?
   a. ______________________________
8. Which setting puts an operating system in hibernate mode when it shuts down?
   a. ______________________________
9. Ensure that the USB selective suspend setting is enabled in your advanced power plan settings.
10. Close all Power Options-related windows.

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 1

Topic: Control Panel Utilities

Subtopics: Power Plans; Hibernate; Sleep, Suspend, and Standby; Power Plan Settings; USB Selective Suspend

Objectives covered

1 Operating Systems

1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility

1.4.14 Power options

1.4.14.1 Hibernate

1.4.14.2 Power plans

1.4.14.3 Sleep/suspend

1.4.14.4 Standby

1.4.14.5 Choose what closing the lid does

1.4.14.6 Turn on fast startup

1.4.14.7 Universal Serial Bus (USB) selective suspend

Ease of Access

Ease of Access is a means by which those with accessibility needs have an easier time performing basic computing tasks, specifically regarding vision, hearing, dexterity, and focus.

Purpose

Upon completing this project, you will better understand Ease of Access options on a device and their role in making computing more accessible.

Steps for Completion

1. On a Windows device, open the Control Panel.
2. Open the Ease of Access Center.
3. Turn off the Always read this section aloud option.
4. Name at least three settings that help those with vision assistance needs when enabled:
    a. ______________________________
    ____
    ____
5. What type of keyboard can help those who cannot use a traditional keyboard?
    a. ______________________________
6. Name at least three settings that help those who need help focusing on tasks:
    a. ______________________________
    ____
    ____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Control Panel Utilities
Subtopic: Ease of Access

Objectives covered
1 Operating Systems
1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility
1.4.15 Ease of Access

Domain 1:

Lesson 8

A+ (220-1102)

Windows Settings Part 1

As each new edition of Windows is released, the Settings area is used more than the Control Panel for configuring Windows Settings. While the Control Panel is still present, the Settings area offers more configurations and customizations than the Control Panel.

Purpose

Upon completing this and the next project, you will better understand commonly used settings in the Windows Settings area.

Steps for Completion

1. On a Windows device, open the Settings area.
2. Access the Time & Language area.
3. Set the time zone to be set automatically.
4. Access the Update and Security area.
5. Change the active hours of your device to reflect the hours of the day you are most active on your device.
6. Access the Personalization area.
7. Change the background picture on your device.
8. Access the Apps area.
9. Uninstall an app you no longer need.
10. Access the Privacy area.
11. Under App permissions, access the Location settings.
12. Clear the location history on your device.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Windows Settings
Subtopics: Time and Language; Update and Security; Personalization; Apps; Privacy

Objectives covered
1 Operating Systems
1.5 Given a scenario, use the appropriate Windows settings
1.5.1 Time & Language
1.5.2 Update & Security
1.5.3 Personalization
1.5.4 Apps
1.5.5 Privacy

Windows Settings Part 2

As mentioned in the previous project, Windows, with each new edition, features more configuration and customization settings in the Settings area, making the Control Panel a less popular choice for configuration options than in previous Windows editions.

Purpose

Upon completing the previous project and this project, you will better understand the configuration and customization options available in the Windows Settings area.

Steps for Completion

1. On a Windows device, open the Settings area.
2. Navigate to the System area.
3. Under Notifications and actions, turn off notifications for apps from which you no longer need notifications.
4. Navigate to the Devices area. How many audio devices are listed?
   a. ______________________________
5. Navigate to the Network and Internet area. What type of connection is in use to connect to the internet?
   a. ______________________________
   ____
6. Navigate to the Gaming area.
7. If the Xbox Game Bar is enabled, disable it.
8. Navigate to the Accounts area.
9. Where can one find the list of accounts used by other apps?
   a. ______________________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1
Topic: Windows Settings
Subtopics: System Settings; Devices; Network and Internet; Gaming; Accounts

Objectives covered

1 Operating Systems
1.5 Given a scenario, use the appropriate Windows settings
1.5.6 System
1.5.7 Devices
1.5.8 Network & Internet
1.5.9 Gaming
1.5.10 Accounts

Domain 1:

Lesson 9

A+ (220-1102)

Workgroup vs. Domain Setup

A Windows device, when first installed, is on a workgroup type of network, even if it is the only device in that workgroup. A workgroup is a peer-to-peer based network with no central server of authority.

A domain contains a server that is a central point for user accounts and their settings. It also controls resource permissions centrally and can set policies for all devices within the domain.

Purpose

Upon completing this project, you will understand how resources are accessed through workgroups and domains. NOTE: You will need access to a printer you can configure and a shared folder on another device.

Steps for Completion

1. On a Windows device, open the properties of the Student folder.
2. Share the folder with the Users group, giving the group read/write permissions.
3. Is a dedicated file server more likely to be found on a workgroup or domain?

    a. ______________________________

4. Access the Printers and Scanners area.
5. Share one of your printers, taking the default name for the printer.
6. If you have access to a shared folder on another device, map that folder to your device as a network drive.

Project Details

Project file

Student folder

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: Client Networking Features

Subtopics: Shared Resources and File Servers; Printers; Mapped Drives

Objectives covered

1 Operating Systems

1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop

1.6.1 Workgroup vs. domain setup

1.6.1.1 Shared resources

1.6.1.2 Printers

1.6.1.3 File servers

1.6.1.4 Mapped drives

Local OS Firewall Settings

Technicians can set up firewalls to filter traffic for entire networks or per device. On a local device, it is crucial to make sure that a firewall, if used, is turned on for a device for both internal (private) and external (public) networks and, if applicable, for domains.

Purpose

Upon completing this project, you will better understand how to ensure that local firewall settings are correct for a device.

Steps for Completion

1. On a Windows device, open Windows Defender Firewall for Advanced Security.
2. For each network type, indicate whether the firewall is on or off:
    a. Public: ______________________________
    b. Private: ______________________________
    c. Domain (if applicable): ______________________________
3. Open port 1433 for TCP for inbound connections for all firewalls, naming the rule **Allow SQL Server**

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Client Networking Features
Subtopics: Firewall Restrictions and Exceptions; Firewall Configuration

Objectives covered
1 Operating Systems
1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop
1.6.2 Local OS firewall settings
1.6.2.1 Application restrictions and exceptions
1.6.2.2 Configuration

LearnKey

Client Network Configuration – Part 1

One key area of support for technicians is to know the IP addressing scheme for the networks they support. A device may need an IP address quickly to start doing work. Technicians need to know whether IP addresses are assigned statically or dynamically, what the DNS server addresses are for the network, and the subnet mask for the network, as the subnet mask determines the size of a network.

Purpose

Upon completing this project, you will better understand configuring a client device to join a network.

Steps for Completion

1. On a Windows device, open the window that shows the network connections on the device.
2. View the details of the live network connection and fill in the following information:
   a. IP address: ______________________________
   b. DNS server: ________________
   c. Subnet mask: ___________________________
   ____
3. Which command-line command will display the IP address of a device?
   a. ______________________________________
4. Which command-line command will display a device's IP address and DNS servers?
   a. ______________________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Client Networking Features
Subtopics: IP Addressing Schemes; DNS; Subnet Mask

Objectives covered
1 Operating Systems
1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop
1.6.3 Client network configuration
1.6.3.1 Internet Protocol (IP) addressing scheme
1.6.3.2 Domain Name System (DNS)
1.6.3.3 Subnet mask

Domain 1:
Lesson 10

A+ (220-1102)

Client Network Configuration – Part 2

To know how to set up client network configurations, a technician needs to know the default gateway for a device. The default gateway, a router, provides a connection to outside networks, assuming a device is on a private network. Virtually all devices needing support will be on a private network.

A technician also needs to know if an IP address is assigned statically or dynamically, and if dynamic, what is the source for the DHCP server for the IP address? Also, a technician needs to know which devices in a network have static IP addresses and why those IP addresses are static.

Purpose

Upon completing this project, you will better understand how to configure IP addresses and their settings on client devices.

Steps for Completion

1. On a Windows device, open the window that will allow you to view the current network connections on the device.
2. View the details of a live network connection. What is the default gateway IP address?
    a. ______________________________
3. Access the IPv4 properties of the network connection. Is the network connection static or dynamic?
    a. ______________________________
4. If the IP address is dynamic, what is the IP address of the DHCP server that leased the IP address to the device?
    a. ______________________________
5. Which devices on a network should have static IP addresses?
    a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Client Networking Features
Subtopic: Gateway and Addressing Types

Objectives covered
1 Operating Systems
1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop
1.6.3 Client network configuration
1.6.3.4 Gateway
1.6.3.5 Static vs. dynamic

LearnKey

Establishing Network Connections

Different networks have different types of connections. Technicians need to know, within a business, what types of networks are in use, specifically as it pertains to wired and wireless networks. Some homes and businesses use both, and some use just one or the other.

For external network connections, many homes and businesses use cable or DSL for internet, but some will use a direct wireless connection to a provider, known as a wireless wide area network (WWAN).

Purpose

Upon completing this project, you will better understand network connections that may need to be established in a home or business.

Steps for Completion

1. On a Windows device, open the VPN settings.
2. Start the process of adding a VPN connection.
3. For creating a new VPN connection, which VPN type uses a pre-shared key?
    a. ____________________
4. Close any open VPN-related windows.
5. Open the area that shows the network adapters you have on your device. Is the network connection you are using wired or wireless?
    a. ____________________
6. Most wired network connections obtain an IP address from which type of server?
    a. ____________________
7. What must be enabled on a cellular device to host a WWAN connection?
    a. ____________________

Project Details

Project file

N/a

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: Client Networking Features

Subtopics: VPN; Wireless Connection; Wired Connection; WWAN

Objectives covered

1 Operating Systems

1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop

1.6.4 Establish network connections

1.6.4.1 Virtual private network (VPN)

1.6.4.2 Wireless

1.6.4.3 Wired

1.6.4.4 Wireless wide area network (WWAN)

Other Client Network Features

Once network connections are established, other client network features can be implemented to better secure network devices and increase network functionality. For example, devices on a public network should not have their data shared, lest the data becomes easy to steal.

Purpose

Upon completing this project, you will better understand how to use client network features to further secure a network.

Steps for Completion

1. What needs to be set up in a web browser's settings to handle internet requests on a client's behalf?
   a. ______________________________
2. On a Windows device, open the Network and Sharing Center.
3. Is your device on a public network or private network?
   a. ______________________________
4. On which type of network should resources not be shared by default?
   a. ______________________________
5. Open File Explorer.
6. In the Network area, how many devices are available for navigation?
   a. ______________________________
7. Open the Wi-Fi settings on the current device. Which feature needs to be enabled to limit the amount of data transferred per month?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Client Networking Features
Subtopics: Proxy Settings; Public vs. Private Networks; File Explorer Navigation; Metered Connections and Limitations

Objectives covered
1 Operating Systems
1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop
1.6.5 Proxy settings
1.6.6 Public network vs. private network
1.6.7 File Explorer navigation – network paths
1.6.8 Metered connections and limitations

Domain 1:
Lesson 11

A+ (220-1102)

App System Requirements

To succeed with an app one wants to use, the system hosting the app must fulfill, at a minimum, the app's system requirements. If an app is installed on a system that lacks resources, the app will perform poorly or not at all. System requirements can address CPU, RAM, hard drive space, and the GPU on a device if one exists.

Purpose

Upon completing this project, you will better understand how to find system requirements for an app and determine if a system meets those requirements.

Steps for Completion

1. What is the maximum amount of RAM a 32-bit app can access?
   a. ______________________________
2. Where can one decide, if available, whether to use an integrated or dedicated graphics card on a device?
   a. ______________________________
3. On a web browser, search for and find the webpage that displays the Windows system requirements for Adobe After Effects.
4. What is the minimum amount of VRAM needed for After Effects?
   a. ______________________________
5. What is the minimum amount of RAM needed for After Effects?
   a. ______________________________
6. What is the CPU requirement for After Effects?
   a. ______________________________
7. How much hard disk space does After Effects require?
   a. ______________________________
8. What does an external hardware token contain that helps with the authentication process?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 1
Topic: App Installs and Configurations
Subtopics: 32-Bit vs. 64-Bit Dependencies; Graphics Card Types; Video and Physical RAM; CPU and Storage Requirements; External Hardware Tokens

Objectives covered
1 Operating Systems
1.7 Given a scenario, apply application installation and configuration concepts
1.7.1 System requirements for applications
1.7.1.1 32-bit vs. 64-bit dependent application requirements
1.7.1.2 Dedicated graphics card vs. integrated
1.7.1.3 Video random-access memory (VRAM) requirements
1.7.1.4 RAM requirements
1.7.1.5 Central processing unit (CPU) requirements
1.7.1.6 External hardware tokens
1.7.1.7 Storage requirements

LearnKey

OS Requirements for Apps and Distribution Methods

Along with system requirements, apps have operating system requirements as, for example, many newer apps will not work with older operating systems. And a 32-bit operating system can only run 32-bit apps even if the device hosting the operating system is a 64-bit operating system.

Most apps, for years, were distributed and installed using CDs or DVDs. However, most apps are attainable by other means nowadays.

Purpose

Upon completing this project, you will better understand possible compatibility problems with apps and how apps are distributed and installed.

Steps for Completion

1. Search for the webpage containing the Windows system requirements for Adobe After Effects on a web browser.
2. What edition of Windows is required for After Effects?
   a. ______________________________
   ____
3. In which folder on Windows are most 32-bit apps installed?
   a. ______________________________
4. Besides DVD, what are two other means by which apps can be obtained?
   a. ______________________________
   b. ______________________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: App Installs and Configurations

Subtopics: Application to OS Compatibility; 32-Bit vs. 64-Bit OS; Physical vs. Downloadable Media; ISO Mountable

Objectives covered

1 Operating Systems

1.7 Given a scenario, apply application installation and configuration concepts

1.7.2 OS requirements for applications

1.7.2.1 Application to OS compatibility

1.7.2.2 32-bit vs. 64-bit OS

1.7.3 Distribution methods

1.7.3.1 Physical media vs. downloadable

1.7.3.2 ISO mountable

App Impact Considerations

Installing an app will impact any device as the app needs device resources to perform. Such an installation could cause performance problems on a device or with other apps on the device. The device itself is not the only resource impacted, however.

Purpose

Upon completing this project, you will better understand the impact considerations that need to be made when installing an app on a device.

Steps for Completion

1. What performance measurements on a device need consideration for being impacted due to an app installation on that device?
   a. ______________________________
   ____
2. Which tool is often used to monitor these measurements?
   a. ______________________________
3. Which tool in Windows can show the impact an installation has on network performance?
   a. ______________________________
4. What do company employees need to be trained on, besides an app, when an app is installed corporate-wide?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: App Installs and Configurations
Subtopic: New App Considerations

Objectives covered
1 Operating Systems
1.7 Given a scenario, apply application installation and configuration concepts
1.7.4 Other considerations for new applications
1.7.4.1 Impact to device
1.7.4.2 Impact to network
1.7.4.3 Impact to operation
1.7.4.4 Impact to business

Domain 1:
Lesson 12

A+ (220-1102)

LearnKey

Workstation Operating Systems

Though Windows is the most popular workstation operating system, there are other operating systems, each with unique and useful features for those who want to use operating systems besides Windows. Technicians need to know the features of each operating system so they can provide recommendations on which operating systems people should use.

Purpose

Upon completing this project, you will better understand the differences among popular workstation operating systems.

Steps for Completion

1. Which version of Windows is not available to all devices running Windows 10?
   a. ____________________
2. Which desktop operating system is known for being open source?
   a. ____________________
3. Which desktop operating system is popular with people in the graphic design industry?
   a. ____________________
4. Which operating system is browser-based?
   a. ____________________
5. Where is data in Chrome OS stored by default?
   a. ____________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: OS Types and Their Purposes

Subtopics: Windows; Linux; macOS, Chrome OS

Objectives covered

1 Operating Systems

1.8 Explain common OS types and their purposes

1.8.1 Workstation OSs

1.8.1.1 Windows

1.8.1.2 Linux

1.8.1.3 macOS

1.8.1.4 Chrome OS

LearnKey

Cell Phone and Tablet Operating Systems

Cell phone and tablet operating systems are centered around lower processor usage than desktop operating systems. And cell phone and tablet operating systems are built for touch rather than the use of a mouse to help navigate the system and its apps.

Purpose

Upon completing this project, you will better understand the features of the major cell phone and tablet operating systems.

Steps for Completion

1. Which Apple-based OS runs on screens large enough to compare to desktop-sized apps?
   a. ______________________________
2. What is one characteristic of the Settings area in Android devices?
   a. ______________________________
3. Which smartphone-based OS is a closed OS?
   a. ______________________________
4. List each official app store for the following operating systems:
   a. Android: ______________________________
   b. iOS: ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: OS Types and Their Purposes
Subtopics: iPadOS; iOS; Android

Objectives covered
1 Operating Systems
1.8 Explain common OS types and their purposes
1.8.2 Cell phone/tablet OSs
1.8.2.1 iPadOS
1.8.2.2 iOS
1.8.2.3 Android

Types of File Systems

Different operating systems have different file systems, each with limitations in file size and partition size. However, with newer file systems, one will probably never reach those limitations with data or a partition as a whole. Most file systems are exclusive to their relative operating systems, but there is one file system that can have its files read across Windows, Linux, and macOS devices.

Purpose

Upon completing this project, you will better understand file systems, their characteristics, and the operating systems to which they belong.

Steps for Completion

1. Which version number of macOS and higher uses APFS as its file system?
   a. ______________________
2. Name three features supported on NTFS that are not supported on FAT32:
   a. ______________________
   b. ______________________
   c. ______________________
3. How many subdirectories does the ext3 file system support?
   a. ______________________
4. How many subdirectories does the ext4 file system support?
   a. ______________________
5. Which file system allows one to save files in Windows and have them be seen on a Linux device?
   a. ______________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1
- **Topic**: OS Types and Their Purposes
  - **Subtopics:** NTFS; FAT32 and exFAT; Ext3 and Ext4; APFS

Objectives covered

1 Operating Systems
- **1.8** Explain common OS types and their purposes
  - **1.8.3** Various file system types
    - **1.8.3.1** New Technology File System (NTFS)
    - **1.8.3.2** File Allocation Table 32 (FAT32)
    - **1.8.3.3** Third extended filesystem (ext3)
    - **1.8.3.4** Fourth extended filesystem (ext4)
    - **1.8.3.5** Apple File System (APFS)
    - **1.8.3.6** Extensible File Allocation Table (exFAT)

doe

Vendor and Compatibility Issues

Two more aspects of operating systems technicians need to be well-versed in are end-of-life (EOL) and compatibility concerns between operating systems. For example, if an app critical to a business works on one operating system, does the same app work on a different operating system? If not, is there a similar app that can be used that can co-exist with the original app?

Purpose

Upon completing this project, you will better understand vendor and compatibility issues related to operating systems.

Steps for Completion

1. Why should an operating system no longer be used when it reaches the EOL stage?
    a. ______________________________
    ____
    ____
2. Using a web browser, search online for the answer to this question: What is the EOL for Windows 10?
    a. ______________________________
3. What is the end date for Windows 10, version 21H2?
    a. ______________________________
4. Search online for the requirements webpage for Adobe After Effects. On which operating systems can After Effects be installed?
    a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: OS Types and Their Purposes
Subtopics: EOL and Update Limitations; Compatibility Concerns Between OSs

Objectives covered
1 Operating Systems
1.8 Explain common OS types and their purposes
1.8.4 Vendor life-cycle limitations
1.8.4.1 End-of-life (EOL)
1.8.4.2 Update limitations
1.8.5 Compatibility concerns between OSs

Domain 1:

Lesson 13

A+ (220-1102)

OS Installations

Operating system installations are no longer just done using CDs or DVDs. With the advent of high-speed downloads, an operating system can be obtained from a parent company's website and configured as needed to be installed on devices using multiple media options.

Purpose

Upon completing this project, you will understand the different ways operating systems are installed on devices. NOTE: To complete this project fully, you will need the installation media for Windows 10, which you can download and create here: Download Windows 10 (microsoft.com)

Steps for Completion

1. What external media methods are available for installing Windows 10?
   a. ______________________________
   b. ______________________________
   c. ______________________________
2. What is the file format of an installation file that is equivalent to that found on optical media?
   a. ______________________________
3. Five devices in a business need the same image for a Windows installation. What method should be used to complete the installations as quickly as possible?
   a. ______________________________
4. Open the Disk Management tool on your device. Is there a hard drive partition that contains Windows installation files?
   a. ______________________________
5. Use the link in the Purpose section to download and create installation media for Windows 10.

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 1
Topic: OS Installations
Subtopics: USB, Optical, SSD, External Boot; Network, Internet-Based Boot; Internal Hard Drive Partition

Objectives covered
1 Operating Systems
1.9 Given a scenario, perform OS installations and upgrades in a diverse OS environment
1.9.1 Boot methods
1.9.1.1 USB
1.9.1.2 Optical media
1.9.1.3 Network
1.9.1.4 Solid-state/flash drives
1.9.1.5 Internet-based
1.9.1.6 External/hot-swappable drive
1.9.1.7 Internal hard drive (partition)

OS Upgrades

Upgrades to operating systems can be done in-place, meaning files, folders, and settings are kept as an operating system is upgraded from one edition of an operating system to another. An upgrade can also be done as a clean install where nothing from the previous installation is preserved. The latter is done when there is no clear upgrade path from a current operating system edition to a new edition.

Technicians can perform upgrades using most of the same installation media options as available for brand-new installations of an operating system.

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 1
Topic: OS Installations
Subtopics: Recovery, Repair, Remote Installations; Types of Image Deployments

Objectives covered

1 Operating Systems
1.9 Given a scenario, perform OS installations and upgrades in a diverse OS environment
1.9.2 Types of installations
1.9.2.1 Upgrade
1.9.2.2 Recovery partition
1.9.2.3 Clean install
1.9.2.4 Image deployment
1.9.2.5 Repair installation
1.9.2.6 Remote network installation
1.9.2.7 Other considerations
1.9.2.7.1 Third-party drivers

Purpose

Upon completing this project, you will better understand how to upgrade an operating system.

Steps for Completion

1. When running a repair installation of Windows, what are two ways an image can be pulled and used to reinstall Windows?
    a. ____________________
    b. ____________________
2. Which type of upgrade preserves a device's files, settings, and apps?
    a. ____________________
3. Which type of Windows installation does not preserve a device's files, settings, and apps?
    a. ____________________
4. True or False: An ISO file can contain multiple images of an operating system.
    a. ____________________
5. A technician wants to install third-party drivers on a device while installing Windows. Where do the drivers need to be located?
    a. ____________________

LearnKey

Drive Partitioning and Formats

Physical hard drives can have multiple partitions, some of which can be used to store system recovery files or host different operating systems. Partitions can be resized as needed to accommodate the need for data to be stored on a partition separate from the main partition of a hard drive.

Technicians should try to decide early in a system's life how hard drives will be partitioned, as the more data on a disk drive, the more challenging it is to change the partition setup on that drive.

Purpose

Upon completing this project, you will better understand the role partitioning has on a hard drive.

Steps for Completion

1. For each drive partition format, list the number of partitions allowed on a hard drive with that format:
   a. GPT: ____________________
   b. MBR: ____________________
2. Open the Disk Management tool on a Windows device.
3. Which partition format is applied to drive 0 on the current device?
   a. ____________________
4. What is the maximum partition size of an MBR partition format?
   a. ____________________
5. If you have unallocated disk space, format it using the NTFS format.

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1
Topic: OS Installations
Subtopics: Partitioning; Drive Format

Objectives covered

1 Operating Systems
1.9 Given a scenario, perform OS installations and upgrades in a diverse OS environment
1.9.3 Partitioning
1.9.3.1 GUID [globally unique identifier] Partition Table (GPT)
1.9.3.2 Master boot record (MBR)
1.9.4 Drive format

LearnKey

Upgrades and Updates

When an operating system is upgraded, special consideration must be given to the current data and settings on the device being upgraded. Data and settings may need to be preserved. A system needs to be examined to make sure it is compatible with a new version of an operating system. And, if another upgrade is coming, should a proposed upgrade occur, or should one wait for the next upgrade?

Purpose

Upon completing this project, you will better understand the considerations that need to be made for possible operating system upgrades and updates.

Steps for Completion

1. What should be backed up on a device before an operating system is upgraded?
   a. ______________________________
2. What specific folder needs to be backed up before an upgrade takes place?
   a. ______________________________
3. If possible, an app built for Windows 7 needs to run on Windows 10. If the default settings do not work for the app, where can some settings be changed that could help the app run?
   a. ______________________________
   ____
4. Check Windows Update for any feature updates ready to be installed on your device (you do not need to run those updates now). How many feature updates are ready to be installed?
   a. ______________________________
5. On a web browser, access this website: Partner Center (microsoft.com)
6. Search for a hardware product you own for compatibility with Windows 10.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: OS Installations
Subtopics: Backup Files and User Preferences; App and Driver Support; Hardware Compatibility; Feature Updates

Objectives covered
1 Operating Systems
1.9 Given a scenario, perform OS installations and upgrades in a diverse OS environment
1.9.5 Upgrade considerations
1.9.5.1 Backup files and user preferences
1.9.5.2 Application and driver support/backward compatibility
1.9.5.3 Hardware compatibility
1.9.6 Feature updates
1.9.6.1 Product life cycle

Domain 1:
Lesson 14

A+ (220-1102)

Mac App Installs

Windows installations primarily use .exe and .msi files to run installations. macOS has different file types for app installations. Knowing these file types helps ensure that only legitimate apps are installed on macOS-based systems.

Furthermore, Apple devices can access a store for downloading and installing apps safely.

Purpose

Upon completing this project, you will better understand file formats for macOS installation files and the uninstallation process for macOS apps.

Steps for Completion

1. Which macOS file is a basic installation file?
   a. ______________________________
2. Which macOS file brings up a wizard-like interface for an installation?
   a. ______________________________
3. What does a .app file typically contain?
   a. ______________________________
4. What is the name of the official store in which people can get apps for a macOS device safely?
   a. ______________________________
5. How can an app be deleted within macOS?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: macOS Tools and Features
Subtopic: App Installs

Objectives covered
1 Operating Systems
1.10 Identify common features and tools of the macOS/desktop OS
1.10.1 Installation and uninstallation of applications
1.10.1.1 File types
1.10.1.1.1 dmg
1.10.1.1.2 pkg
1.10.1.1.3 App
1.10.1.2 App Store
1.10.1.3 Uninstallation process

LearnKey

Apple IDs and Best Practices

Apple IDs are used to synchronize data among devices, similar to what is done with Microsoft accounts for Windows devices. Apple IDs can be used in both personal and corporate settings.

With macOS devices, there is a set of best practices for keeping the devices healthy from both an operating system and app standpoint. Technicians should know these best practices so that they can help maintain the health of these devices.

Purpose

Upon completing this project, you will better understand the role of an Apple ID and best practices for maintaining macOS devices.

Steps for Completion

1. A business wants to have Apple IDs for its employees and control what can be done with them. What type of Apple IDs should be created?
   a. ______________________________
2. Name two utilities that can be used to back up data from a macOS device:
   a. ______________________________
   b. ______________________________
3. What role does XProtect have on a macOS device?
   a. ______________________________
4. What steps can one take to check for system updates on a macOS device?
   1. ______________________________
   2. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: macOS Tools and Features
Subtopics: Apple IDs; Backups; Antivirus; Updates and Patches

Objectives covered
1 Operating Systems
1.10 Identify common features and tools of the macOS/desktop OS
1.10.2 Apple ID and corporate restrictions
1.10.3 Best practices
1.10.3.1 Backups
1.10.3.2 Antivirus
1.10.3.3 Updates/patches

Mac System Preferences

The System Preferences area on a macOS device is the central point for configuration options for the device. Within System Preferences, one can install devices, set privacy and accessibility settings, and control backup options for the device. Technicians should know the configuration options available within System Preferences to help end-users be more productive with their macOS devices.

Purpose

Upon completing this project, you will better understand the configuration options available within System Preferences.

Steps for Completion

1. Which display feature changes a Mac's color scheme to warmer after dark?
   a. ______________________________
2. Which types of network connections should appear automatically in the Network window?
   a. ______________________________
3. Which printer window shows the available ink levels on a printer?
   a. ______________________________
4. True or False: All scanners need to be installed on Mac devices.
   a. ______________________________
5. Which System Preference allows one to control location tracking for a device?
   a. ______________________________
6. Name at least two of the sections of tools available in the Accessibility System Preference:
   a. ____
   ____
7. Which System Preference is used to set up the backup of an entire hard drive?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 1
Topic: macOS Tools and Features
Subtopics: Displays; Networks; Printers and Scanners; Privacy Settings; Accessibility; Time Machine

Objectives covered
1 Operating Systems
- **1.10** Identify common features and tools of the macOS/desktop OS
  - **1.10.4** System preferences
    - **1.10.4.1** Displays
    - **1.10.4.1** Networks
    - **1.10.4.3** Printers
    - **1.10.4.4** Scanners
    - **1.10.4.5** Privacy
    - **1.10.4.6** Accessibility
    - **1.10.4.7** Time machine

macOS Features – Part 1

The next three projects will touch on specific macOS features, which, like System Preferences, are meant to enhance one's productivity on a macOS device. Technicians need a cursory knowledge of these features to help support people who use macOS devices.

The most important takeaway for the exam is knowing when and how these features are used.

Purpose

After completing this project and the following two projects, you will better understand the features of a macOS system.

Steps for Completion

1. Which feature allows one to work with multiple desktops on a Mac?
   a. ______________________________
2. Name three categories of information that Keychain can store:
   a. ______________________________
   b. ______________________________
   c. ______________________________
3. In which window is Keychain found?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Operating Systems
Subtopics: Multiple Desktops, Mission Control; Keychain

Objectives covered
1 Operating Systems
1.10 Identify common features and tools of the macOS/desktop OS
1.10.5 Features
1.10.5.1 Multiple desktops
1.10.5.2 Mission Control
1.10.5.3 Keychain

Domain 1:

Lesson 15

A+ (220-1102)

LearnKey

macOS Features – Part 2

macOS features do not stop with desktop control features and keychains. macOS features allow people to search terms in multiple places, organize their files and folders, and, for devices that do not have a DVD player, connect to one that does. Technicians need to know at least these features and what they do, even if they are not used daily.

Purpose

Upon completing the previous project, this project, and the next project, you will better understand macOS features.

Steps for Completion

1. Which macOS feature allows one to store contacts, files, and other information in the cloud?
   a. ____________________
2. Which macOS feature allows one to control actions taken depending upon a finger combination used on a touchpad?
   a. ____________________
3. Which macOS feature is a toolbar that holds open apps and can be configured to hold shortcuts for apps, folders, and files?
   a. ____________________
4. Which macOS feature organizes files, folders, and apps on a hard drive?
   a. ____________________
5. A person needs to install an app from a DVD and does not have a DVD player available on a device. Which feature allows for using a DVD player on someone else's device?
   a. ____________________
6. From where does Spotlight return search results on a topic?
   a. ____________________
   ____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: macOS Tools and Features
Subtopics: Spotlight; iCloud; Gestures; Finder, Remote Disc; Dock

Objectives covered
1 Operating Systems
1.10 Identify common features and tools of the macOS/desktop OS
1.10.5 Features
1.10.5.4 Spotlight
1.10.5.5 iCloud
1.10.5.6 Gestures
1.10.5.7 Finder
1.10.5.8 Remote Disc
1.10.5.9 Dock

LearnKey

macOS Features – Part 3

Some macOS features work with security, commands, and preservation of a system when one app stops functioning. This project is the third of three projects on macOS features. For the exam and real-life support, be aware of these different features and when they are used, even if you do not support devices with macOS regularly.

Purpose

Upon completing the previous two projects and this project, you will better understand macOS features and their uses.

Steps for Completion

1. What are two features of the Disk Utility tool?

   a. ______________________________
   ____
   ____
   ____
   ____

2. Within Disk Utility, which tool is used to repair a drive?

   a. ______________________________

3. Which tool is a disk encryption service within macOS?

   a. ______________________________

4. In which app are command-line commands run on a Mac?

   a. ______________________________

5. An app is hanging within macOS. What tool can be used to close the app?

   a. ______________________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: macOS Tools and Features

Subtopics: Disk Utility; FileVault; Terminal; Force Quit

Objectives covered

1 Operating Systems

1.10 Identify common features and tools of the macOS/desktop OS

1.10.6 Disk Utility

1.10.7 FileVault

1.10.8 Terminal

1.10.9 Force Quit

Domain 1:
Lesson 16

A+ (220-1102)

Linux Commands – Part 1

As is the case with Windows, Linux has a command-line tool called Terminal that can be used to run commands, either individually or as part of a script. Some of these commands have similar names to the equivalent commands in Windows, and some do not.

For this project and the following two projects, having access to an installation of Linux is highly beneficial as that will allow you to practice the commands covered in these projects. The projects themselves will cover which commands are used given certain situations.

Purpose

Upon completing this project and the next two projects, you will better understand Linux commands and their uses.

Steps for Completion

1. Which Linux command gives help on a specific command and its usage?
   a. ______________________________
2. Which Linux command lists folders and files within a directory?
   a. ______________________________
3. A technician needs to know the current directory in which the technician is working. What command should they run?
   a. ______________________________
4. A technician runs the following command on a file: **chmod u+rw**. What has happened to the file?
   a. ______________________________
5. Name the command used for each of these file tasks:
   a. Copy a file: ______________________________
   b. Move a file: ______________________________
   c. Delete a file: ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Linux Tools and Features
Subtopics: Ls and Man; Pwd; Mv, Cp, Rm; Chmod

Objectives covered
1 Operating Systems
1.11 Identify common features and tools of the Linux client/desktop OS
1.11.1 Common commands
1.11.1.1 ls
1.11.1.2 pwd
1.11.1.3 mv
1.11.1.4 cp
1.11.1.5 rm
1.11.1.6 chmod
1.11.1.15 man

Linux Commands – Part 2

Some Linux commands require owner-type permissions to run, similar to running an elevated command prompt in Windows. Other Linux commands find specific text within a file. And some commands are used to install files and apps on a device. You will explore these types of commands in this project.

Purpose

Upon completing this project, you will know more about the roles of command-line commands within Linux.

Steps for Completion

1. A technician wants to make a different user the owner of a file. Which command accomplishes this task?
   a. ______________________________
2. Which command switches users within the Terminal window?
   a. ______________________________
3. A command needs to be run with a superuser designation. Which keyword, placed before a command, adds that designation?
   a. ______________________________
4. Which command/attribute combination displays a routing table on a device?
   a. ______________________________
5. Which command shows the amount of disk space left on a drive?
   a. ______________________________
6. A technician needs to find the word, health, in a file named script2. What should the technician type at the command line to accomplish this task?
   a. ______________________________
7. What does the find command specifically find?
   a. ______________________________
8. What are the two commands used to download and install packages, depending upon the version of Linux one has?
   a. ______________________________
   b. ______________________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1

Topic: Linux Tools and Features

Subtopics: Chown, Su/sudo; Apt-get, Yum; Ip; Df; Grep, Find

Objectives covered

1 Operating Systems

1.11 Identify common features and tools of the Linux client/desktop OS

1.11.1 Common commands

1.11.1.7 chown

1.11.1.8 su/sudo

1.11.1.9 apt-get

1.11.1.10 yum

1.11.1.11 ip

1.11.1.12 df

1.11.1.13 grep

1.11.1.17 find

Domain 1:

Lesson 17

A+ (220-1102)

LearnKey

Linux Commands – Part 3

The last of the three projects of Linux commands will focus on commands that show DNS information, contents of files, and even open a built-in editor for files.

As with the previous two projects, having a Linux installation to practice with is key to learning these commands well. Again, knowing when to use each command is essential for the exam and real-life Linux-based support situations.

Purpose

Upon completing this project, you will, along with completing the previous two projects, better understand Linux commands and their uses.

Steps for Completion

1. What two DNS-related items does the dig command show when dig is run by itself?
   a. ____________________
   b. ____________________
2. Which command shows processes a user is running?
   a. ____________________
3. Which command shows running processes and allows one to kill a process?
   a. ____________________
4. Which command shows the contents of a file?
   a. ____________________
5. What does the nano command do on Linux devices that have nano installed?
   a. ____________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 1
Topic: LInux Tools and Features
Subtopics: Ps; Top; Dig; Cat, Nano

Objectives covered

1 Operating Systems
1.11 Identify common features and tools of the Linux client/desktop OS
1.11.1 Common commands
1.11.1.14 ps
1.11.1.16 top
1.11.1.18 dig
1.11.1.19 cat
1.11.1.20 nano

Linux Best Practices

As with Windows and macOS, Linux has a set of best practices one should follow for maintaining a Linux device. While the concepts are the same, the tools used for these best practices differ.

In addition to best practices, Linux has tools that make file sharing possible with Windows devices.

Purpose

Upon completing this project, you will know more about Linux best practices and how to enable Linux to host shares that Windows devices can see.

Steps for Completion

1. Which command can be used to initiate a remote backup on a Linux device?
   a. ______________________________
2. True or False: Linux devices typically have built-in antivirus/antimalware protection.
   a. ______________________________
3. Depending upon one's version of Linux, which two commands can get packages needed to keep Linux up to date with the latest updates and patches?
   a. ______________________________
   b. ______________________________
4. Which shell is the most popular shell in Linux?
   a. ______________________________
5. What is the name of the program used to run commands in a command-line interface in Linux?
   a. ______________________________
6. What is the primary protocol Linux uses for sharing files and folders?
   a. ______________________________
7. Which Linux tool supports SMB for sharing files and folders with Windows devices?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Linux Tools and Features
Subtopics: Linux Backups; Linux Antivirus; Linux Updates/Patches; Shell/Terminal

Objectives covered
1 Operating Systems
1.11 Identify common features and tools of the Linux client/desktop OS
1.11.2 Best practices
1.11.2.1 Backups
1.11.2.2 Antivirus
1.11.2.3 Updates/patches
1.11.3 Tools
1.11.3.1 Shell/terminal
1.11.3.2 Samba

Domain 2:
Lesson 1

A+ (220-1102)

LearnKey

Physical Security Measures

Safeguarding an IT infrastructure begins with physical security measures, specifically, meaning security for a building. Security measures protect everything from outside a building to the devices within.

Purpose

Upon completing this project, you will better understand physical security measures.

Steps for Completion

1. Which security measure is a room between two security doors, one going outside and the other into a secure building?
    a. ______________________
2. List two advantages of using badges and badge readers:
    a. ______________________
    ____
    b. ______________________
    ____
3. In addition to cameras, what else does video surveillance use?
    a. ______________________
    ____
4. Which security measure keeps a building secure after hours, alerting a security team when someone attempts to enter a building?
    a. ______________________
5. What is a vibration sensor?
    a. ______________________
    ____
6. Which equipment lock is used for locking a laptop to a desk to prevent theft?
    a. ______________________
7. What is one of the most significant benefits of using security guards?
    a. ______________________
    ____
8. List two security measures that are both physical and psychological deterrents:
    a. ______________________
    b. ______________________

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 2
Topic: Security Measures
Subtopics: Access Control Vestibule; Badge Reader; Video Surveillance; Alarm Systems; Motion Sensors; Door Locks: Equipment Locks; Guards; Bollards and Fences

Objectives covered
2 Security
2.1 Summarize various security measures and their purposes
2.1.1 Physical security
2.1.1.1 Access control vestibule
2.1.1.2 Badge reader
2.1.1.3 Video surveillance
2.1.1.4 Alarm systems
2.1.1.5 Motion sensors
2.1.1.6 Door locks
2.1.1.7 Equipment locks
2.1.1.8 Guards
2.1.1.9 Bollards
2.1.1.10 Fences

Physical Staff Security

Physical staff security involves having staff use devices to verify their authorization when entering secure areas. Staff security devices can range from a key fob to more complex biometrics. Key fobs are small security tokens programmed to fit an individual's access needs. Biometrics uses a person's unique characteristics to create a form of authentication that cannot be stolen or replicated.

Purpose

Upon completing this project, you will become more familiar with physical staff security.

Steps for Completion

1. Label the following statement as true or false.
    a. ________________ Data from key fobs can be logged, allowing security to review who has been where and when.
2. What do many smart cards require with authentication?
    a. ____
    ____
    ____
3. What weakness do keys and keylocks have regarding security?
    a. ____
    ____
4. List two types of biometrics:
    a. ____
    ____
    ____
5. What type of camera sensor detects physical activity even in the dark?
    a. ____
6. Why would a magnetometer be used on people exiting a building?
    a. ____
    ____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Security Measures
Subtopics: Key Fobs; Smart Cards; Keys; Biometrics; Lighting; Magnetometers

Objectives covered
2 Security
2.1 Summarize various security measures and their purposes
2.1.2 Physical security for staff
2.1.2.1 Key fobs
2.1.2.2 Smart cards
2.1.2.3 Keys
2.1.2.4 Biometrics
2.1.2.4.1 Retina scanner
2.1.2.4.2 Fingerprint scanner
2.1.2.4.3 Palmprint scanner
2.1.2.5 Lighting
2.1.2.6 Magnetometers

Domain 2:

Lesson 2

A+ (220-1102)

LearnKey

Logical Security

Logical security, in the context of IT infrastructure, does not involve a physical building or physical areas within a building. Instead, logical security consists of software safeguards for an organization's infrastructure. The principle of least privilege is a tenet applied to logical security that ensures people have access to the resources they need for completing their jobs, but nothing more.

Purpose

Upon completing this project, you will better understand different types of logical security.

Steps for Completion

1. How does the principle of least privilege keep resources secure?

   a. ______________________________
   ____

2. Label the following statement as true or false.

   a. ____________ ACLs only apply to files, folders, and users.

3. What is the risk of using email to receive an authentication code?

   a. ______________________________
   ____
   ____

4. What advantage does a soft token have over a hard token?

   a. ______________________________
   ____

5. List two ways of receiving an authentication code on a cellphone:

   a. ______________________________

   b. ______________________________

6. What is the advantage of using an authenticator application for multifactor authentication (MFA)?

   a. ______________________________
   ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 2

Topic: Security Measures

Subtopics: Principle of Least Privilege; Access Control Lists; Multifactor Authentication; Email; Hard Token; Soft Token; SMS and Voice Call; Authenticator Application

Objectives covered

2 Security

2.1 Summarize various security measures and their purposes

2.1.3 Logical security

2.1.3.1 Principle of least privilege

2.1.3.2 Access control lists (ACLs)

2.1.3.3 Multifactor authentication (MFA)

2.1.3.4 Email

2.1.3.5 Hard token

2.1.3.6 Soft token

2.1.3.7 Short message service (SMS)

2.1.3.8 Voice call

2.1.3.9 Authenticator application

LearnKey

Mobile Device Management

Management of mobile devices is an important security factor in a business. Mobile device management (MDM) includes determining which mobile devices are allowed on a network, which apps are allowed on those devices, and the policies put in place. These policies ensure that mobile devices meet compliance standards to be on a network and determine what will happen if a device becomes lost or stolen.

Purpose

Upon completing this project, you will better understand mobile device management.

Steps for Completion

1. What can an MDM help prevent?
   a. ____
   ____
2. What is Microsoft Endpoint Manager?
   a. ____
3. Label the following statement as true or false.
   a. ______________________________ MDM offers a way to organize and secure mobile devices on a network.
4. What does MDM use to control access for devices on a network?
   a. ____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Security Measures
Subtopic: Mobile Device Management

Objectives covered
2 Security
2.1 Summarize various security measures and their purposes
2.1.4 Mobile device management (MDM)

Active Directory

Active Directory provides administrators with a central point in a network for storing users, groups, and their attributes. Active Directory allows administrators to set Group Policy for every device in a domain and apply different policies to different groups within that domain. One aspect of Active Directory is the use of logon scripts to automate processes for users. Another aspect is Organizational Units (OUs), which admins utilize to organize users and groups.

Purpose

Upon completing this project, you will become more familiar with Active Directory.

Steps for Completion

1. How do logon scripts save administrators time?

   a. ____
   ____
   ____

2. What is the advantage of using a domain?

   a. ____
   ____

3. Which Active Directory mechanism's purpose is to control the rights of devices and how they function?

   a. ____

4. How can Organizational Units (OUs) help administrators in an organization with hundreds of computers?

   a. ____

5. What is the benefit of a home folder for administrators?

   a. ____
   ____

6. List two things folder redirection helps save:

   a. ____

   b. ____

7. Label the following statement as true or false.

   a. ____________________ Security groups can save administrators time and minimize errors in controlling account permissions within a domain.

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 2
Topic: Security Measures
Subtopics: Logon Script; Domain; Group Policy and Updates; Organizational Units; Home Folder; Folder Redirection; Security Groups

Objectives covered
2 Security
2.1 Summarize various security measures and their purposes
2.1.5 Active Directory
2.1.5.1 Logon script
2.1.5.2 Domain
2.1.5.3 Group Policy/updates
2.1.5.4 Organizational units
2.1.5.5 Home folder
2.1.5.6 Folder redirection
2.1.5.7 Security groups

Domain 2:
Lesson 3

A+ (220-1102)

Wireless Security Protocols and Encryption

The two newest wireless security protocols provide strong encryption for wireless networks. Wi-Fi Protected Access 2 (WPA2) uses 128-bit encryption to protect data from attackers and a pre-shared key for authentication.

The newest wireless security protocol is Wi-Fi Protected Access 3 (WPA3). WPA3 also uses 128-bit encryption for personal mode but a stronger 192-bit encryption for enterprise mode. Rather than a pre-shared key, WPA3 uses the Simultaneous Equals exchange (SAE) for faster authentication than WPA2.

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 2

Topic: Wireless Security Protocols

Subtopics: WPA2 and AES; WPA3 and TKIP

Objectives covered

2 Security

2.2 Compare and contrast wireless security protocols and authentication methods

2.2.1 Protocols and encryption

2.2.1.1 Wi-Fi Protected Access 2 (WPA2)

2.2.1.2 WPA3

2.2.1.3 Temporal Key Integrity Protocol (TKIP)

2.2.1.4 Advanced Encryption Standard (AES)

Purpose

Upon completing this project, you will better understand wireless security protocols and encryption.

Steps for Completion

1. Label the following statement as true or false.
   a. ______________________ WPA is more secure than WPA2.
2. SAE is resistant to what type of attacks?
   a. ____
3. What type of authentication does WPA2 use?
   a. ____
4. What is the older wireless security protocol still available on wireless access points?
   a. ____
5. Why should WPA only be used if WPA2 and WPA3 are not available?
   a. ____
   ____
6. Which wireless security protocol uses the Advanced Encryption Standard (AES)?
   a. ____
7. Which wireless security protocol is considered the most secure?
   a. ____

Authentication Methods

Enterprise Wi-Fi enables users to connect to a network on a business property rather than a home or residential property. The Enterprise Security setting uses a different form of authentication than personal Wi-Fi. First, Remote Authentication Dial-In User Service (RADIUS) is a centralized source for controlling an enterprise wireless network's authentication, authorization, and accounting.

Terminal Access Controller Access Control System (TACACS+) is a protocol similar to RADIUS but developed by Cisco to be used exclusively with their products. However, TACACS+ is now used on other devices to authenticate routers and managed switches.

Purpose

Upon completing this project, you will become more familiar with authentication methods.

Steps for Completion

1. Label the following statement as true or false.
    a. ________________ RADIUS stores usernames on every wireless access point within a network.
2. Label the following statement as true or false.
    a. __________ TACACS+ can be an authentication mechanism for wireless networks connecting to a corporate network.
3. What is the most significant benefit of Kerberos?
    a. ____
    ____
4. Why do systems use multifactor authentication?
    a. ____
5. List two tasks users must sometimes complete for multifactor authentication.
    a. ____
    b. ____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Wireless Security Protocols
Subtopics: RADIUS and TACACS+; Kerberos; Multifactor

Objectives covered
2 Security
2.2 Compare and contrast wireless security protocols and authentication methods
2.2.2 Authentication
2.2.2.1 Remote Authentication Dial-In User Service (RADIUS)
2.2.2.2 Terminal Access Controller Access-Control System (TACACS+)
2.2.2.3 Kerberos
2.2.2.4 Multifactor

Domain 2:
Lesson 4

A+ (220-1102)

Viruses

Malicious software, or malware, comes in many forms that must be recognized, removed, and prevented. One type of malware is a virus or block of malicious code. Viruses require a carrier to propagate through a system or multiple systems. Some viruses morph to avoid antivirus software, while others hide from it. Multipartite viruses affect various components such as programs, files, and boot sectors.

Purpose

Upon completing this project, you will become more familiar with common forms of viruses.

Steps for Completion

1. What type of virus hides from antivirus software?
    a. ____________________
2. How can one avoid malware when downloading and installing software?
    a. ____________________
    ____
3. Why should users never launch an executable file from an email?
    a. ____________________
4. What is a common type of carrier for viruses in Microsoft Word?
    a. ____________________
5. What is the best way to combat a boot sector virus?
    a. ____________________
6. How does Secure Boot ensure that a boot process has not been modified?
    a. ____________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Malware
Subtopics: Trojan; Virus; Boot Sector Virus

Objectives covered
2 Security
2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods
2.3.1 Malware
2.3.1.1 Trojan
2.3.1.3 Virus
2.3.1.7 Boot sector virus

Other Malware

Viruses are common types of malware, but users should be aware of malware in many other forms, including spyware, ransomware, rootkits, keyloggers, and cryptomining. Spyware is a form of malware that allows attackers to spy on people as they navigate through apps, webpages, or similar items. Another very costly form of malware is ransomware, which steals data, encrypts it, and holds it for ransom.

A rootkit is a type of malware that is masked and enables access to off-limits areas. Once it obtains access, a rootkit will cause damage and take over a computer's root or administration areas. A keylogger is a tool to capture keystrokes typed on a keyboard so an attacker can use them maliciously.

Purpose

Upon completing this project, you will become more familiar with common forms of malware.

Steps for Completion

1. What should users do before running antivirus software to find a rootkit?
   a. ______________________________
   ____
2. When installing software, what should users look for to avoid installing spyware?
   a. ______________________________
   ____
3. Which type of malware is so prevalent and destructive to normal business operations that many antimalware packages have files dedicated to stopping it?
   a. ______________________________
4. What type of keyloggers do attackers rarely use?
   a. ______________________________
5. What is not malware but can cause high energy bills and wear out computer components?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Malware
Subtopics: Rootkit; Spyware; Ransomware; Keylogger; Cryptominers

Objectives covered
2 Security
2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods
2.3.1 Malware
2.3.1.2 Rootkit
2.3.1.4 Spyware
2.3.1.5 Ransomware
2.3.1.6 Keylogger
2.3.1.8 Cryptominers

Malware Removal

Several tools are available for removing malware from a system. One of the first measures against a potential malware attack is scanning a device with an installed antivirus or antimalware app. Recovery mode provides other options for fighting malware if scanning does not work. Users can run a startup repair, uninstall updates, restore the OS to a previous point, or recover Windows with an image file. When other means of eradicating malware have failed, recovery mode provides a place where users can reinstall an operating system.

Purpose

Upon completing this project, you will better understand malware removal tools.

Steps for Completion

1. What should one check before running antimalware or antivirus software on a device?
   a. ______________________________
   ____
2. How does one reboot a system into Windows recovery mode?
   a. ______________________________
   ____
3. Label the following statement as true or false.
   a. ______________ Backing up important files before reinstalling an OS is unnecessary.
4. When is the only time a device infected with malware should connect to a network?
   a. ______________________________
5. List the two options available when one resets a PC:
   a. ______________________________
   b. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Malware
Subtopics: Recovery Mode; Antivirus and Antimalware; OS Reinstallation

Objectives covered
2 Security
2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods
2.3.2 Tools and methods
2.3.2.1 Recovery mode
2.3.2.2 Antivirus
2.3.2.3 Antimalware
2.3.2.7 OS reinstallation

LearnKey

Malware Prevention

In addition to eradicating malware from a system, it is essential to prevent future malware attacks. Malware prevention tools include software firewalls, anti-phishing training, and user education regarding common threats. Software firewalls can prevent malware by blocking malicious traffic from entering a network. Education and anti-phishing training prevent malware by helping users identify suspicious emails and other possible attacks.

Purpose

Upon completing this project, you will better understand some methods for preventing malware.

Steps for Completion

1. What is the first checkpoint on a firewall?
   a. ______________________________
   ____
2. What is one way to recognize a suspicious email?
   a. ______________________________
   ____
   ____
3. List two ways to educate employees about malware.
   a. ______________________________
   ____
   ____
   ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 2
Topic: Malware
Subtopics: Software Firewalls; Anti-Phishing Training; Educating Users on Common Threats

Objectives covered

2 Security
2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods
2.3.2 Tools and methods
2.3.2.4 Software firewalls
2.3.2.5 Anti-phishing training
2.3.2.6 User education regarding common threats

Domain 2:

Lesson 5

A+ (220-1102)

LearnKey

Forms of Phishing

Social engineering is the act of deceiving and manipulating someone into sharing personal information for malicious use. One form of social engineering that many people fall victim to is phishing. Phishing occurs when attackers attempt to gain someone's personal information through deceptive emails. Several other social engineering techniques are different forms of phishing.

Purpose

Upon completing this project, you will become more familiar with different forms of phishing.

Steps for Completion

1. Label the following statement as true or false.
   a. ______________________________ Reputable organizations often send direct links via email to sign in to a site.
2. What is spear phishing?
   a. ____
   ____
3. Which form of phishing uses Voice over IP (VoIP) to gain information from people?
   a. ____
4. How is whaling different from phishing?
   a. ____
5. How can a company prevent impersonation attempts?
   a. ____
   ____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Social Engineering
Subtopics: Phishing; Vishing; Whaling; Tailgating; Impersonation;

Objectives covered
2 Security
2.4 Explain common social-engineering attacks, threats, and vulnerabilities
2.4.1 Social engineering
2.4.1.1 Phishing
2.4.1.2 Vishing
2.4.1.4 Whaling
2.4.1.6 Impersonation

LearnKey

Other Social Engineering

Some other forms of social engineering are not related to phishing. Shoulder surfing is a social engineering technique where an attacker peers over a victim's shoulder to steal information. A more subtle form of social engineering is tailgating, which involves an unauthorized individual entering a secure area by following behind someone with legitimate authorization.

Sometimes, throwing out documents into a dumpster is an invitation to have information stolen. Dumpster diving is searching garbage for intact papers containing data attackers can use to exploit a security weakness. Another form of social engineering specific to wireless networks is an evil twin. An evil twin is a wireless access point set up to mimic an existing wireless access point with the same service set identifier (SSID).

Purpose

Upon completing this project, you will better understand other forms of social engineering.

Steps for Completion

1. What is an effective tool for blocking shoulder surfing attempts?
   a. ______________________________
2. List two mitigation techniques against tailgating:
   a. ______________________________
   b. ______________________________
   ____
3. How can one deter dumpster diving?
   a. ______________________________
4. List two ways to avoid an evil twin.
   a. ______________________________
   b. ______________________________
   ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 2
Topic: Social Engineering
Subtopics: Shoulder Surfing; Tailgating; Dumpster Diving; Evil Twin

Objectives covered

2 Security
2.4 Explain common social-engineering attacks, threats, and vulnerabilities
2.4.1 Social engineering
2.4.1.3 Shoulder surfing
2.4.1.5 Tailgating
2.4.1.7 Dumpster diving
2.4.1.8 Evil twin

Domain 2:

Lesson 6

A+ (220-1102)

LearnKey

Network and Device Attacks

Technicians should be aware of several common attacks on devices and networks. An attack that disrupts or halts a network's production and services is known as a DoS attack. When multiple devices carry out this type of attack, it is known as a DDoS attack.

Another type of attack is password cracking, which means stealing someone's password. The two main types of password attacks that technicians should know are the brute force attack and the dictionary attack. A brute force attack involves repeatedly guessing a password to crack it, while a dictionary attack means using dictionary words to crack a password.

Purpose

Upon completing this project, you will become more familiar with attacks on devices and networks.

Steps for Completion

1. What type of attack is a ping flood attack?
   a. ____________________
2. What is the name of the attacking computers created by zombies in a DDoS attack?
   a. ____________________
3. What is a zero-day attack?
   a. ____________________
   ____
   ____
4. Label the following statement as true or false
   a. ____________________. There is no real way to prevent a zero-day attack.
5. What command can help a technician spot spoofing attacks?
   a. ____________________
6. Where might an on-path attack occur?
   a. ____________________
   ____
7. How can one make a brute-force attack on their password more difficult?
   a. ____________________
8. How can a dictionary attack be avoided?
   a. ____________________

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 2
Topic: Social Engineering
Subtopics: DoS and DDoS; Zero-Day Attack; Spoofing; On-Path Attack; Brute-Force Attack; Dictionary Attack

Objectives covered
2 Security
2.4 Explain common social-engineering attacks, threats, and vulnerabilities
2.4.2 Threats
2.4.2.1 Distributed Denial of service (DDoS)
2.4.2.2 Denial of service (DoS)
2.4.2.3 Zero-day attack
2.4.2.4 Spoofing
2.4.2.5 On-path attack
2.4.2.6 Brute-force attack
2.4.2.7 Dictionary attack

Other Threats

One of the most common threats to infrastructure is an insider threat, defined as a security risk caused by someone within an organization. This insider is often a disgruntled employee who has left or is just leaving an organization. Another threat to infrastructure is a Structured Query Language (SQL) injection. An SQL injection is a technique attackers use to gain unauthorized access to a web application database.

Purpose

Upon completing this project, you will better understand some other infrastructure threats.

Steps for Completion

1. Label the following statement as true or false.
   a. ______________________ An insider threat is a problem because an insider does not usually need to hack into a system.
2. How might a company minimize the chance of insider threats?
   a. ______________________________________
   ____
   ____
3. List the two main steps an organization can take to prevent SQL injections:
   a. ______________________________________
   b. ______________________________________
   ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 2
Topic: Social Engineering
Subtopics: Insider Threat; SQL Injection

Objectives covered

2 Security
2.4 Explain common social-engineering attacks, threats, and vulnerabilities
2.4.2 Threats
2.4.2.8 Insider threat
2.4.2.9 Structured Query Language (SQL) injection

Vulnerabilities

Vulnerabilities are areas of an infrastructure that can become threats if not addressed. A system that does not meet policy requirements to be allowed on a network is called a non-compliant system and is vulnerable to attacks. Non-compliant systems include unprotected systems and those running end-of-life (EOL) operating systems (OSs).

Purpose

Upon completing this project, you will become more familiar with vulnerabilities in an infrastructure.

Steps for Completion

1. Label the following statement as true or false.

   a. ______________ Non-compliant devices risk spreading malware throughout a network.

2. What is the risk of allowing unpatched devices on a network?

   a. ____

   ____

3. List two things to check in the Windows Security and Virus threat protection area of a system:

   a. ____

   b. ____

   ____

4. Why are EOL OSs considered a vulnerability?

   a. ____

   ____

   ____

   ____

5. How can a mobile device management (MDM) tool help mitigate a BYOD vulnerability?

   a. ____

   ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 2

Topic: Social Engineering

Subtopics: Non-Compliant and Unpatched Systems; Unprotected Systems; EOL Operating Systems; BYOD

Objectives covered

2 Security

2.4 Explain common social-engineering attacks, threats, and vulnerabilities

2.4.3 Vulnerabilities

2.4.3.1 Non-compliant systems

2.4.3.2 Unpatched systems

2.4.3.3 Unprotected systems (missing antivirus/missing firewall)

2.3.4.4 EOL OSs

2.3.4.5 Bring your own device (BYOD)

Domain 2:

Lesson 7

A+ (220-1102)

Defender Antivirus and Firewall

One should always ensure an activated security package is installed and enabled on a system. If no third-party antimalware tool is in use, it is essential to ensure the built-in antivirus program, if one is present, is enabled. Having an antimalware package activated and making sure the definitions are up to date is crucial to protecting a system. A firewall is also crucial because it can help prevent malicious traffic from entering a network, but only if activated. While most firewalls control network traffic based on ports and protocols, they can also use an application as the criterion to control inbound or outbound traffic.

Purpose

Upon completing this project, you will better understand Microsoft Defender Antivirus.

Steps for Completion

1. What should a user always do before running antimalware?

   a. ______________________________

2. When is the only time one should deactivate built-in virus and threat protection?

   a. ______________________________
   ____

3. When might one deactivate a firewall?

   a. ______________________________
   ____

4. Which ports should one consider closing in a business?

   a. ______________________________
   ____

5. What happens when too many unnecessary apps are allowed on a network?

   a. ______________________________
   ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 2
- **Topic**: Windows Security Settings
  - **Subtopics:** Activate Defender; Updated Definitions; Activate Firewall; Port Security; Application Security

Objectives covered

2 Security
- **2.5** Given a scenario, manage and configure basic security settings in the Microsoft Windows OS
  - **2.5.1** Defender Antivirus
    - **2.5.1.1** Defender Antivirus
    - **2.5.1.2** Updated definitions
  - **2.5.2** Firewall
    - **2.5.2.1** Activate/deactivate
    - **2.5.2.2** Port Security
    - **2.5.2.3** Application Security

Users and Groups

One aspect of managing a Windows-based system is administering its users and groups. A technician providing support to a Windows device should discern whether the primary user or users are signing in with local or Microsoft accounts. A Microsoft account allows users to synchronize data and settings across devices, while local accounts do not. Several accounts are available on a Windows 10 device, including a Standard account, an Administrator account, a Guest User, and a Power User.

Purpose

Upon completing this project, you will become more familiar with users and groups.

Steps for Completion

1. What prevents all businesses from using Microsoft accounts for their employees?

    a. ____

    ____

    ____

2. What program does Windows use to synchronize data and settings across devices?

    a. ____

3. Why should the Guest and default Administrator accounts be disabled in Windows?

    a. ____

    ____

4. Which account can create and manage files and folders but cannot change settings or permissions for users?

    a. ____

5. What is the only reason Windows includes a Power Users group?

    a. ____

    ____

6. Label the following statement as true or false.

    a. __________________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Windows Security Settings
Subtopics: Local vs. Microsoft Account; Standard vs. Administrator Account; Guest User; Power User

Objectives covered
2 Security
2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS
2.5.3 Users and groups
2.5.3.1 Local vs. Microsoft account
2.5.3.2 Standard account
2.5.3.3 Administrator
2.5.3.4 Guest user
2.5.3.3 Power user

Domain 2:

Lesson 8

A+ (220-1102)

Login OS Options

Operating systems offer several different sign-in options for users. A username and password is an easy way to set up authentication in Windows. Microsoft recommends using a personal identification number (PIN) because it is easier to remember than a password. Fingerprints and facial recognition are two methods of authentication using biometrics. Another authentication option is single sign-on (SSO), which allows users to sign in to a system once and access multiple areas.

Purpose

Upon completing this project, you will better understand OS sign in options.

Steps for Completion

1. What is the downside to using a username and password as authentication?
    a. ______________________________
2. A PIN is easier to remember than a username and password, but what is its downside?
    a. ______________________________
    ____
3. What are biometrics?
    a. ______________________________
    ____
4. What is the benefit of using fingerprint and facial recognition over other sign-in options?
    a. ______________________________
5. What does SSO help lower?
    a. ______________________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 2
Topic: Windows Security Settings
Subtopics: Username, Password, PIN; Fingerprint and Facial Recognition; SSO

Objectives covered

2 Security
2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS
2.5.4 Login OS Options
2.5.4.1 Username and password
2.5.4.2 Personal identification number (PIN)
2.5.4.3 Fingerprint
2.5.4.4 Facial recognition
2.5.4.5 Single sign-on (SSO)

NTFS vs. Share Permissions

The permissions assigned to users and groups for files and folders depend on the file system one uses. FAT32 only provides Read and Read/Write permissions for folders and files. In contrast, NTFS file systems have numerous permissions to assign to users and groups, including complete control of a folder.

Files and folders inherit permissions by default from a parent folder or drive. Inheritance may sometimes lead to users having more permissions than needed to do their job. In an NTFS file system, an admin can follow the principle of least privilege and remove specific unnecessary permissions for these users.

Purpose

Upon completing this project, you will better understand different file system permissions.

Steps for Completion

1. Navigate to the Signature Files folder within your Student folder.
2. Use the Security tab to edit permissions and add a group named **stresstest**.
3. Give the stresstest group the Modify permission.
4. Disable inheritance on the folder. Ensure inherited permissions are converted into explicit permissions on the folder.
5. Remove permissions for users on the folder.
6. What does it mean to break inheritance on a folder?
    a. ____
    ____
7. How can breaking inheritance make a device more secure?
    a. ____
    ____
8. What is one reason to use NTFS instead of FAT32 as a file system?
    a. ____
9. Label the following statement as true or false.
    a. __________ FAT32 provides Modify and Full Control permissions to folders and files.

Project Details

Project file
Signature Files Folder

Estimated completion time
10 minutes

Video reference
Domain 2
Topic: Windows Security Settings
Subtopics: File and Folder Attributes; Inheritance

Objectives covered
2 Security
2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS
2.5.5 NTFS vs. share permissions
2.5.5.1 File and folder attributes
2.5.5.2 Inheritance

User Account Control

User Account Control (UAC) is a Windows feature that sets user authorization levels. Setting authorization levels includes prompting standard users to be elevated to administrator mode when apps require it. UAC can block apps from automatically installing and help users prevent accidental changes to a system.

Purpose

Upon completing this project, you will become more familiar with User Account Control.

Steps for Completion

1. What is the default setting for User Account Control (UAC)?

   a. ______________________________
   ____

2. Which system app needs to run in administrator mode?

   a. ______________________________
   ____

3. When might one consider setting UAC to Always notify?

   a. ______________________________
   ____

4. Label the following statement as true or false.

   a. ______________________________ UAC prompts users every time an app is installed.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Windows Security Settings
Subtopics: UAC

Objectives covered
2 Security
2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS
2.5.6 Run as administrator vs. standard user
2.5.6.1 User Account Control (UAC)

Data Encryption Features

Windows provides several encryption features for protecting data, such as BitLocker, BitLocker to Go, and Encrypting File System (EFS). BitLocker allows users to encrypt an entire hard drive and protect data by making the drive inaccessible without a key. BitLocker to Go works the same, except it uses encryption on external drives, such as removable USB drives. The EFS feature encrypts select folders on a hard drive rather than encrypting the entire drive.

Purpose

Upon completing this project, you will become more familiar with data encryption features.

Steps for Completion

1. Navigate to the onlinescripts folder within your Student folder.
2. Encrypt the contents of the folder.
3. Why is the best use of EFS on devices with multiple users?
   a. ______________________________
   ____
   ____
4. List two options for unlocking a drive encrypted by BitLocker to Go:
   a. ______________________________
   b. ______________________________
5. Why might it be more important to encrypt data on external than internal drives?
   a. ______________________________
6. Label the following statement as true or false.
   a. ____________________ One should back up a decryption key to the same drive as the encrypted folder to which it is assigned.

Project Details

Project file
onlinescripts folder

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Windows Security Settings
Subtopics: BitLocker and BitLocker To Go; EFS

Objectives covered
2 Security
2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS
2.5.7 BitLocker
2.5.8 BitLocker To Go
2.5.9 Encrypting File System (EFS)

Domain 2:
Lesson 9

A+ (220-1102)

LearnKey

Data Storage and Password Best Practices

As part of workstation security, data at rest should be encrypted. Windows devices offer two encryption options: BitLocker and Encrypting File System (EFS).

Workstation security also includes passwords. Password complexity requirements, expiration requirements, and BIOS or UEFI passwords can help keep a business's IT environment secure.

Purpose

Upon completing this project, you will better understand encryption options for stored data and password best practices.

Steps for Completion

1. ____________________ encrypts entire hard drives.
2. ____________________ encrypts files and folders.
3. List two important characteristics of complexity requirements for passwords. ____
4. According to CompTIA's recommendation, how many characters should a password be? ____
5. What can technicians do to prevent brute-force attacks on users' passwords?
   a. ____
   ____
6. What action requires an administrator password to be entered before the action can be performed?
   a. ____
   ____
7. What action requires a user password to be entered before the action can be performed?
   a. ____
   ____

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 2
Topic: Workstation Best Practices
Subtopic: Data-at-Rest; Password Complexity Requirements; Expiration Requirements; BIOS/UEFI Passwords

Objectives covered
2 Security
2.6 Given a scenario, configure a workstation to meet best practices for security
2.6.1 Data-at-rest encryption
2.6.2 Password best practices
2.6.2.1 Complexity requirements
2.6.2.2 Expiration requirements
2.6.2.3 Basic input/output system (BIOS)/ Unified Extensible Firmware Interface (UEFI) passwords

End-User Best Practices

End-user practices are an important consideration when maintaining a secure IT environment. Some end-user best practices include using a screensaver lock, signing off a device, securing mobile hardware, and securing sensitive information. Using these best practices can help prevent attacks and data theft on a network.

Purpose

Upon completing this project, you will better understand end-user best practices.

Steps for Completion

1. Why should a user that spends time away from their device use a screensaver lock?

   a. ______________________________

2. Why can logging a device off when it is not in use be better than using a screensaver lock?

   a. ______________________________

3. When a user is not taking an easily moved device with them, what should be used on the device while they are away?

   a. ______________________________

4. Personally identifiable information (PII) should only be disclosed ______________ and through secure channels.

5. Why should one avoid holding a credit card out in the open?

   a. ______________________________

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 2

Topic: Workstation Best Practices

Subtopic: Screensaver Locks; Signing Off when not in Use; Secure Hardware, PII, and Passwords

Objectives covered

2 Security

2.6 Given a scenario, configure a workstation to meet best practices for security

2.6.3 End-user best practices

2.6.3.1 Use screensaver locks

2.6.3.2 Log off when not in use

2.6.3.3 Secure/protect critical hardware (e.g., laptops)

2.6.3.4 Secure personally identifiable information (PII) and passwords

If time permits, have students discuss how they would communicate these best practices to end users.

Account Management

User accounts are essential to a business's IT environment, and technicians need to know how to manage those accounts to keep them secure. There are several measures technicians can implement to help ensure users' activities do not lead to security threats.

Purpose

Upon completing this project, you will better understand how to keep accounts secure.

Steps for Completion

1. Determine whether each statement is true or false. Use T for true and F for false.

    a. __________ A user should have every available permission unless a permission interferes with the user's work.

    b. __________ Reducing the time a user account can be signed in reduces the chances of someone using the account for malicious activity.

    c. __________ One can use the net user command to restrict a user's sign in hours.

    d. __________ A user should only use known accounts.

    e. __________ The Guest and Administrator accounts are enabled in Windows 10 by default.

    f. __________ The main purpose of using a failed attempts lockout setting is to discourage hackers from continually trying to sign in to a system.

    g. __________ Using a screen lock is the most effective way to protect a device during a period of inactivity.

    h. __________ Disabling AutoRun prevents drives from working.

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 2
Topic: Workstation Best Practices
Subtopic: Restrict User Permissions; Restrict Sign-In Times; Disable Guest Account; Use Failed Attempts Lockout; Use Timeout/Screen Lock; Change Default Administrator Account; Disable AutoRun; Disable AutoPlay

Objectives covered
2 Security
2.6 Given a scenario, configure a workstation to meet best practices for security
2.6.4 Account management
2.6.4.1 Restrict user permissions
2.6.4.2 Restrict login times
2.6.4.3 Disable guest account
2.6.4.4 Use failed attempts lockout
2.6.4.5 Use timeout/screen lock
2.6.5 Change default administrator's user account/password
2.6.6 Disable AutoRun
2.6.7 Disable AutoPlay

2. Why might a technician choose to rename a known account rather than disable it?

    a. ____
    ____
    ____

3. Why should a technician consider disabling AutoRun?

    a. ____

4. Why should a technician consider disabling AutoPlay?

    a. ____
    ____

Domain 2:

Lesson 10

A+ (220-1102)

Screen Locks

Implementing screen locks on devices helps protect data. Devices without screen locks are easier targets for attackers, as having no screen lock on a device means no authentication is required to access it. Several screen lock options are available to users, including facial recognition, PIN codes, fingerprints, patterns, and swipes.

Purpose

Upon completing this project, you will better understand screen lock options.

Steps for Completion

1. Determine what security level each screen lock type provides. Use 1 for very secure, 2 for somewhat secure, and 3 for not very secure.

    a. __________ PIN codes

    b. __________ Patterns

    c. __________ Facial recognition

    d. __________ Swipes

    e. __________ Fingerprints

2. If you have a mobile device such as a smartphone or tablet, activate a screen lock of your choosing on the device.

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 2

Topic: Securing Mobile Devices

Subtopic: Facial Recognition; PIN Codes and Swipes; Fingerprint and Patterns

Objectives covered

2 Security

2.7 Explain common methods for securing mobile and embedded devices

2.7.1 Screen locks

2.7.1.1 Facial recognition

2.7.1.2 PIN codes

2.7.1.3 Fingerprint

2.7.1.4 Pattern

2.7.1.5 Swipe

Mobile Device Security

Mobile devices have security vulnerabilities, especially because they are prone to being lost or stolen. Technicians should consider the security threats that can occur on mobile devices and decide how to remediate those threats should they occur.

Purpose

Upon completing this project, you will better understand how to keep mobile devices secure.

Steps for Completion

1. When might a user want to perform a remote wipe?
   a. ____
   ____
2. What application can one use on iPhones as a remote locator?
   a. ____
3. Choose an answer to complete each statement.

A. fixes an urgent security vulnerability	C. does not fix an urgent security vulnerability
B. takes a long time	D. takes a short time

   a. If an update ________, then the update can wait.
   b. If an update ________, then the update should happen right away.
4. Many devices ____________________ data automatically when a device is locked.
5. List two cloud storage services that one can use for remote backups. ______________________________
   ____
6. Why might one choose to enable a setting on a mobile device that erases data after a certain number of sign-in attempts have occurred?
   a. ____
   ____
   ____
7. When using antivirus or anti-malware programs, what should be updated regularly? ____________________
8. When might one want to enable a firewall on a mobile device?
   a. ____
   ____
9. To prevent security vulnerabilities on a network, one can use a(n) ____________________ on a smartphone to turn off Internet of Things (IoT) devices that are not in use.

Project Details

Project file
N/A

Estimated completion time
15 minutes

Video reference
Domain 2
Topic: Securing Mobile Devices
Subtopic: Remote Wipes; Locator Applications; OS Updates; Device Encryption; Remote Backup Applications; Failed Login Attempt Restrictions; Antivirus/Antimalware; Firewalls; IoT

Objectives covered
2 Security
2.7 Explain common methods for securing mobile and embedded devices
2.7.2 Remote wipes
2.7.3 Locator applications
2.7.4 OS updates
2.7.5 Device encryption
2.7.6 Remote backup applications
2.7.7 Failed login attempts restrictions
2.7.8 Antivirus/anti-malware
2.7.9 Firewalls
2.7.11 Internet of Things (IoT)

Policies

Allowing employees to use personal devices on a business's network can be useful for efficiency and productivity. However, mobile devices can present security risks to a network. Because of these security risks, businesses that allow personal devices to be used for work should have a bring-your-own-device (BYOD) policy. After implementing a BYOD policy, businesses should enforce the security requirements outlined in the policy.

Purpose

Upon completing this project, you will better understand how to keep a network that uses personal devices for business secure.

Steps for Completion

1. Why is a BYOD policy important for businesses that allow employees to bring their own devices?
   a. ______________________________

2. List two topics that a BYOD policy should cover.
   a. ______________________________

3. How can technicians enforce security requirements outlined in a business's BYOD policy?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: Securing Mobile Devices
Subtopic: BYOD vs. Corporate-Owned Devices; Profile Security Requirements

Objectives covered
2 Security
2.7 Explain common methods for securing mobile and embedded devices
2.7.10 Policies and procedures
2.7.10.1 BYOD vs. corporate owned
2.7.10.2 Profile security requirements

Domain 2:

Lesson 11

A+ (220-1102)

LearnKey

Data Destruction and Repurposing

Businesses possess data that exists in documents and on hard drives. Eventually, this data may no longer be needed. When data is no longer needed, technicians should consider disposal and repurposing methods to ensure the wrong people cannot access data.

Purpose

Upon completing this project, you will better understand how to destroy data on hard drives and documents and how to repurpose a hard drive.

Steps for Completion

1. Determine whether each statement is true or false. Use T for true and F for false.

   a. ________ Formatting a hard drive erases all data on the drive.

   b. ________ One should use a high-quality, cross-cutting paper shredder to destroy documents that are no longer needed.

   c. ________ One should check the regulations in the area before incinerating documents that are no longer needed.

   d. ________ Regardless of the business's industry, all business documents should be destroyed as soon as they are no longer needed.

   e. ________ There is no way to extract data that has been deleted from a hard drive.

2. One can drill holes into the ____________________ of a magnetic hard drive to make data inaccessible on the drive.

3. Describe the process of degaussing a drive.

   a. ____
   ____
   ____

4. What command can be used in Linux to see a list of ways to use the shred command to overwrite data?

   a. ____

5. Match the hard drive formatting type to its description.

A. Low-level formatting	B. Standard formatting

   a. ________ Sets up disk sectors to receive data; normally performed at a factory.

   b. ________ An easy method of formatting a hard drive that a user can perform.

6. What should one obtain when contracting a third-party vendor to destroy data?

   a. ____

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 2

Topic: Data Destruction and Disposal

Subtopic: Drilling; Shredding and Incinerating; Degaussing; Erasing and Wiping; Low-Level and Standard Formatting; Vendors and Certificates of Destruction

Objectives covered

2 Security

- **2.8** Given a scenario, use common data destruction and disposal methods
  - **2.8.1** Physical destruction
    - **2.8.1.1** Drilling
    - **2.8.1.2** Shredding
    - **2.8.1.3** Degaussing
    - **2.8.1.4** Incinerating
  - **2.8.2** Recycling or repurposing best practices
    - **2.8.2.1** Erasing/wiping
    - **2.8.2.2** Low-level formatting
    - **2.8.2.3** Standard formatting
  - **2.8.3** Outsourcing concepts
    - **2.8.3.1** Third-party vendor
    - **2.8.3.2** Certification of destruction/recycling

Router and WAP Settings – Part 1

Setting up a router or a wireless access point on a small office/home office (SOHO) network can differ from setting up a more extensive network. Technicians may choose whether some router and wireless access point settings are enabled based on whether the network is a SOHO network or a larger network. Technicians should be aware of the tools and best practices available to set up a SOHO network to meet users' needs.

Purpose

Upon completing this project, you will better understand router and wireless access point settings on SOHO networks.

Steps for Completion

1. What is the first administrative task one should perform on a wireless access point?
   a. ____________________
2. What type of firewall should be on if no other firewall is active? ____________________
3. ____________ filtering protects a network from both internal and external attacks.
4. What is firmware?
   a. ____________________
   ____
5. What is the purpose of content filtering?
   a. ____________________
   ____
   ____
6. Ideally, where should a wireless access point be located?
   a. ____________________
7. List one item from which wireless access points should be kept away.
   a. ____________________

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 2
Topic: SOHO Network Security Settings
Subtopic: Change Default Passwords; IP Filtering; Firmware Updates; Content Filtering; Physical Placement

Objectives covered
2 Security
2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks
2.9.1 Home router settings
2.9.1.1 Change default passwords
2.9.1.2 IP filtering
2.9.1.3 Firmware updates
2.9.1.4 Content filtering
2.9.1.5 Physical placement/secure locations

LearnKey

Router and WAP Settings – Part 2

Technicians must understand how router and wireless access point settings differ on small office/home office (SOHO) networks compared to more extensive networks. For example, WAN IP address settings should vary based on whether the WAN address is being used on a SOHO or a large network. In addition, Universal Plug and Play (UPnP) should be disabled on large networks but may be appropriate for SOHO networks. Understanding these settings can help technicians set up a secure network while still meeting users' needs.

Purpose

Upon completing this project, you will better understand router and wireless access point settings for SOHO networks.

Steps for Completion

1. Most wireless access points give IP addresses to devices through ____________________.
2. What is a WAN IP address?
   a. ____
   ____
3. Most businesses' WAN IP addresses should be ________________________.
4. What is the purpose of Universal Plug and Play (UPnP)?
   a. ____
   ____
   ____
5. What is a screened subnet?
   a. ____
   ____
6. List a type of server common in screened subnets.
   a. ____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 2
Topic: SOHO Network Security Settings
Subtopic: DHCP Reservations; Static WAN; UPnP; Screened Subnet

Objectives covered
2 Security
2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks
2.9.1 Home router settings
2.9.1.6 Dynamic Host Configuration Protocol (DHCP) reservations
2.9.1.7 Static wide-area network (WAN) IP
2.9.1.8 Universal Plug and Play (UPnP)
2.9.1.9 Screened subnet

Domain 2:

Lesson 12

A+ (220-1102)

Wireless Network Security

When setting up a wireless network, technicians must give significant consideration to how to keep the network secure. Technicians should also know which channels are safe to use on different frequencies. Wireless access points also have firewall settings that technicians should be aware of as they set up a wireless network.

Purpose

Upon completing this project, you will better understand wireless network security.

Steps for Completion

1. Why should one change a default service set identifier (SSID) on a wireless access point?

    a. ____
    ____
    ____

2. What happens when an SSID broadcast is disabled?

    a. ____
    ____
    ____

3. WPA uses ______________ for encryption.
4. WPA2 uses ______________ for encryption.
5. WPA3 uses ______________ for encryption.
6. Which encryption method is more secure, TKIP or AES? ______________
7. How should one keep a guest account secure if one needs to have a guest account enabled?

    a. ____
    ____

8. What channels can be used on 5 GHz frequencies?

    a. 20 MHz channel width: ____

    b. 40 MHz channel width: ____

    c. 80 MHz channel width: ____

9. What channels can be used on 2.4 GHz frequencies in North America? ______________________________
10. Determine whether the statement is true or false. Use T for true and F for false.

    a. _________ Technicians do not need to block unused ports if the setting to do so is not available on a wireless access point's firewall.

11. Wireless access points can accept incoming connections from other networks, but many times, a specific ______________ number is needed for a connection.

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 2

- **Topic**: SOHO Network Security Settings
    - **Subtopic**: Changing the SSID; Disabling SSID Broadcast; Encryption Settings; Disabling Guest Access; Changing Channels; Disabling Unused Ports; Port Forwarding/Mapping

Objectives covered

2 Security

- **2.9** Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks
    - **2.9.2** Wireless specific
        - **2.9.2.1** Changing the service set identifier (SSID)
        - **2.9.2.2** Disabling SSID broadcast
        - **2.9.2.3** Encryption settings
        - **2.9.2.4** Disabling guest access
        - **2.9.2.5** Changing channels
    - **2.9.3** Firewall settings
        - **2.9.3.1** Disabling unused ports
        - **2.9.3.2** Port forwarding/mapping

Domain 2:

Lesson 13

A+ (220-1102)

LearnKey

Web Browsers

When using the internet, users must only access trusted sources. There are many known, trusted sources of web browser downloads and application downloads. In addition, checking to see if a website's certificate is valid is a quick way to assess whether the website one is visiting is secure.

Purpose

Upon completing this project, you will better understand where to find web browsers and how to use them safely.

Steps for Completion

1. Choose an answer to complete each statement.

A. cannot be trusted	B. can be trusted

   a. If two hashes of a file do not match, the file ________________.

   b. If two hashes of a file match, the file ________________.

2. What is a trusted source of web browsers and applications for Apple devices? ________________

3. What is a trusted source of web browsers and applications for Android devices? ________________

4. What is a trusted source of web browsers and applications for Windows devices? ________________

5. From where should one download an extension or plug-in?

   a. ________________
   ____

6. Within a web browser, ________________ to websites a person signs into often can be stored within the browser's settings.

7. How does a certificate ensure a website is secure?

   a. ________________
   ____

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 2

Topic: Install and Configure Browsers

Subtopic: Browser Download and Installation; Extensions and Plug-Ins; Password Managers; Secure Connections and Certificates

Objectives covered

2 Security

2.10 Given a scenario, install and configure browsers and relevant security settings

2.10.1 Browser download/installation

2.10.1.1 Trusted sources

2.10.1.2 Untrusted sources

2.10.2 Extensions and plug-ins

2.10.2.1 Trusted sources

2.10.2.2 Untrusted sources

2.10.3 Password managers

2.10.4 Secure connections/sites – valid certificates

Web Browser Settings

There are several browser settings technicians need to be aware of when configuring and supporting web browsers. Technicians may need to search for these settings to find them, so technicians should be sure to be aware of these settings to be used to better protect a network.

Purpose

Upon completing this project, you will better understand web browser settings.

Steps for Completion

1. What is the purpose of a pop-up blocker?
   a. ____
   ____
2. Determine whether each statement is true or false. Use T for true and F for false.
   a. ________ Browsing data should be cleared from a device when the data is no longer needed.
   b. _________ Private browsing prevents everyone from seeing one's browsing history.
   c. _________ To synchronize browsing history and bookmarks on multiple devices, one must use a Bluetooth connection.
3. In a web browser of your choosing, view the browsing history on your device.
4. What are cached files?
   a. ____
   ____
   ____
5. What is the purpose of private browsing?
   a. ____
   ____
6. What is an example of an ad blocker?
   a. ____

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 2
Topic: Install and Configure Browsers
Subtopic: Pop-Up Blockers; Clearing Browsing Data and Cache; Private Browsing Mode; Sign-In Data Synchronization; Ad Blockers

Objectives covered
2 Security
2.10 Given a scenario, install and configure browsers and relevant security settings
2.10.5 Settings
2.10.5.1 Pop-up blocker
2.10.5.2 Clearing browsing data
2.10.5.3 Clearing cache
2.10.5.4 Private-browsing mode
2.10.5.5 Sign-in browser data synchronization
2.10.5.6 Ad blockers

Domain 3:

Lesson 1

A+ (220-1102)

Windows Issues – Part 1

No operating system is perfect. Operating systems, like Windows, will have occasional issues. The key to solving these issues is to know how to diagnose these issues and make the necessary hardware or software configuration changes to try to mitigate these issues.

Purpose

Upon completing this project, you will better understand how to approach Windows device problems such as the blue screen of death (BSOD), sluggish performance, boot issues, frequent shutdowns, services not starting, and applications crashing.

Steps for Completion

1. On a Windows device, open Event Viewer. How many critical errors have occurred in the past week?
   a. ______________________________
2. Search the Event Viewer for Kernel-Boot and Kernel-General entries. How many of these errors have happened in the last week?
   a. ______________________________
3. Kernel-Boot and Kernel-General errors are indicative of what type of problem?
   a. ______________________________
4. An event with an ID of 7000 indicates which type of problem?
   a. ______________________________
5. A BSOD is classified as which event type in Event Viewer?
   a. ______________________________
6. List two causes of a BSOD:
   a. ______________________________
   b. ______________________________
7. Which tool can help one diagnose sluggish performance on a device?
   a. ______________________________
8. Open the System Configuration tool.
9. Set the system to create a ntblog.txt file the next time the system boots up.
10. An app keeps crashing. What should a technician look for first?
    a. ______________________________

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 3
Topic: Common Windows OS Problems
Subtopics: BSOD; Sluggish Performance; Boot Problems; Frequent Shutdowns; Services not Starting; Applications Crashing

Objectives covered
3 Software Troubleshooting
3.1 Given a scenario, troubleshoot common Windows OS problems
3.1.1 Common symptoms
3.1.1.1 Blue screen of death (BSOD)
3.1.1.2 Sluggish performance
3.1.1.3 Boot problems
3.1.1.4 Frequent shutdowns
3.1.1.5 Services not starting
3.1.1.6 Applications crashing

LearnKey

Windows Issues – Part 2

Some Windows issues are merely warnings, such as when memory is running low or when a process takes longer to load than usual. If warnings are not addressed, they could become issues. This project is the second of two projects covering common Windows issues.

Purpose

Upon completing the previous project and this project, you will better understand Windows issues, how to diagnose them, and how to solve or work around these issues.

Steps for Completion

1. On a Windows device, ensure that the amount of virtual memory available is 1.5 times the amount of RAM installed on the system.
2. Where is virtual memory located on a device?
   a. ______________________________
3. How can one avoid getting USB controller resource warnings?
   a. ______________________________
   ____
   ____
4. Which Windows tool can help diagnose system stability problems?
   a. ______________________________
5. A device, when starting up, shows a message that it cannot find an operating system. What should a technician do first to troubleshoot the problem?
   a. ______________________________
   ____
6. Which types of files can be removed from a roaming profile to speed up the load time of the profile?
   a. ______________________________
   b. ______________________________
7. With what time server is your device synchronizing?
   a. ______________________________

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 3

Topic: Common Windows OS Problems

Subtopics: Low Memory Warnings; USB Controller Resource Warnings; System Instability; No OS Found; Slow Profile Load; Time Drift

Objectives covered

3 Software Troubleshooting

3.1 Given a scenario, troubleshoot common Windows OS problems

3.1.1 Common symptoms

3.1.1.7 Low memory warnings

3.1.1.8 USB controller resource warnings

3.1.1.9 System instability

3.1.1.10 No OS found

3.1.1.11 Slow profile load

3.1.1.12 Time drift

Domain 3:

Lesson 2

A+ (220-1102)

LearnKey

Windows Troubleshooting Part 1

Troubleshooting involves identifying problems, but once they are identified, knowing the first step to take to solve these problems is the most important aspect of resolving them. For example, when is a reboot necessary? When is it not necessary? Over time, technicians learn and sharpen these skills as they gain experience troubleshooting Windows issues.

Purpose

Upon completing this and the next project, you will better understand troubleshooting common Windows operating system problems.

Steps for Completion

1. What are two benefits of rebooting a system to attempt to solve an operating system problem?
   a. ______________________________
   ____
   b. ______________________________
2. List, in the proper order, the two steps one should take if an app crashes often:
   a. ______________________________
   b. ______________________________
3. Which resource is the easiest to add to a device to boost performance?
   a. ______________________________
4. Search for and find the Windows 11 system requirements in a web browser. How much RAM is required?
   a. ______________________________
5. Restart the Spooler service on your device.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 3
Topic: Common Windows OS Problems
Subtopics: Reboot; Restart Services; App Uninstalls and Updates; Add Resources; Verify Requirements

Objectives covered
3 Software Troubleshooting
3.1 Given a scenario, troubleshoot common Windows OS problems
3.1.2 Common troubleshooting steps
3.1.2.1 Reboot
3.1.2.2 Restart services
3.1.2.3 Uninstall/reinstall/update applications
3.1.2.4 Add resources
3.1.2.5 Verify requirements

Windows Troubleshooting Part 2

When rebooting an operating system and other tactics do not solve Windows problems, reinstalling the operating system may be the correct solution. Short of a complete reinstall, a repair might solve a problem. If not, a technician must determine how best to reinstall Windows on a device.

Purpose

Upon completing this project, you will better understand repair options for Windows installations.

Steps for Completion

1. On a Windows device, open an elevated command prompt.
2. Start running a system file check that verifies the integrity of system files.
3. Create a system restore point named **Before Installs**
4. Re-running the Windows setup file while Windows is running will do what to Windows?
    a. ______________________________
5. What does imaging do to a device besides installing Windows?
    a. ______________________________
    ____
6. Which screen within Windows Update allows one to roll back Windows updates?
    a. ______________________________
7. What is the first step in rebuilding a profile on a user account?
    a. ______________________________

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 3

Topic: Common Windows OS Problems

Subtopics: System File Check; Repair Windows; Restore; Reimage; Roll Back Updates; Rebuild Windows Profiles

Objectives covered

3 Software Troubleshooting

3.1 Given a scenario, troubleshoot common Windows OS problems

3.1.2 Common troubleshooting steps

3.1.2.6 System file check

3.1.2.7 Repair Windows

3.1.2.8 Restore

3.1.2.9 Reimage

3.1.2.10 Roll back updates

3.1.2.11 Rebuild Windows profiles

Domain 3:

Lesson 3

A+ (220-1102)

PC Security Issues

Security issues on PCs could be blatant or an underlying cause of what appears to be more common issues on PCs. However, a technician should look to improve security on a device when troubleshooting any type of issue on that device, even if the issue does not seem security-related.

Purpose

Upon completing this project, you will better understand common PC security issues.

Steps for Completion

1. A person cannot make a network connection over a wired network. What should a technician check first?
    a. ______________________________
    ____
2. A person cannot make a network connection over a wireless network. What should a technician check first?
    a. ______________________________
    ____
3. Where do most legitimate desktop alerts appear in Windows?
    a. ______________________________
4. Which app alerts, including antimalware app alerts, should be the only alerts considered legitimate on a device?
    a. ______________________________
5. Which command checks the integrity of system files on a device?
    a. ______________________________
6. If a Windows update fails, what is usually done with the system?
    a. ______________________________

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 3
Topic: Common PC Security Issues
Subtopics: No Network Access; Desktop Alerts; False Antivirus Alerts; Altered System or Personal Files; Unwanted Notifications; OS Update Failures

Objectives covered
3 Software Troubleshooting
3.2 Given a scenario, troubleshoot common personal computer (PC) security issues
3.2.1 Common symptoms
3.2.1.1 Unable to access the network
3.2.1.2 Desktop alerts
3.2.1.3 False alerts regarding antivirus protection
3.2.1.4 Altered system or personal files
3.2.1.4.1 Missing/renamed files
3.2.1.5 Unwanted notifications within the OS
3.2.1.6 OS update failures

LearnKey

Browser Security Issues

Web browsers have security issues independent of security issues found on an operating system. For example, pop-up ads are far more prevalent on web browsers than on desktops. Also, people browsing websites need to ensure that any website to which they send data has proper encryption through a valid certificate.

Purpose

Upon completing this project, you will better understand common browser security issues.

Steps for Completion

1. Make sure the pop-up blocker is enabled on the web browsers you use.
2. What should be done with the device if a browser exhibits many pop-ups after ensuring pop-up blockers are turned on?
    a. ______________________________
3. What is a common cause of a certificate warning on a website?
    a. ______________________________
4. What should one assume with data on a website with an expired certificate?
    a. ______________________________
5. A person gets redirected to what appears to be a malicious website. What should a technician check for first on a network?
    a. ______________________________
    ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 3

Topic: Common PC Security Issues

Subtopics: Random or Frequent Pop-Ups; Certificate Warnings; Redirection

Objectives covered

3 Software Troubleshooting

3.2 Given a scenario, troubleshoot common personal computer (PC) security issues

3.2.2 Browser-related symptoms

3.2.2.1 Random/frequent pop-ups

3.2.2.2 Certificate warnings

3.2.2.3 Redirection

Domain 3:

Lesson 4

A+ (220-1102)

Malware Removal – First Steps

When a technician gets the dreaded notification that malware may be present on a device, there is a series of steps to follow first to ensure malware, if present, does not spread to other devices. Then, within the remediation process on a device, there is another set of steps to follow.

The main rule with malware is to contain it without letting it spread and then do what is needed to mitigate future malware occurrences.

Purpose

Upon completing this project, you will better understand the first steps in the malware removal process.

Steps for Completion

1. Search for, download, and install Process Explorer from Microsoft on a Windows device.
2. Run Process Explorer. Are any processes using an excessive amount of CPU percentage?
   a. ____
3. Once a system is found to have malware, what should be done next with the system?
   a. ____________________________
4. Disable System Restore on your device.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 3
Topic: Malware Removal Best Practices
Subtopics: Investigate and Verify Malware; Quarantine Infected Systems; Disable System Restore

Objectives covered
3 Software Troubleshooting
3.3 Given a scenario, use best practice procedures for malware removal
3.3.1 1. Investigate and verify malware symptoms
3.3.2 2. Quarantine infected systems
3.3.3 3. Disable System Restore in Windows

Remediating Systems

Once a system is quarantined and System Restore is disabled, the remediation process for a device can begin. Before scanning a device, one needs to ensure that the definition files for the antimalware software used for the scan are updated so that the latest malware can be found and eradicated.

Purpose

Upon completing this project, you will better understand how to remediate systems affected by malware.

Steps for Completion

1. On a Windows device, update the definition files for the antimalware software you are using.
2. Run an antimalware scan on your system using the Quick Scan or equivalent settings.
3. If possible, schedule a scan to run weekly.
4. Enable System Restore on your device.
5. Create a restore point, naming it **After Scan**
6. How can a technician educate end users on avoiding malware?
   a. ______________________________
   ____
   ____
   ____
   ____
7. What can be done with a system to run an antimalware scan on it with a minimal amount of drivers loaded on the system?
   a. ______________________________
   ____

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 3
Topic: Malware Removal Best Practices
Subtopics: Update Antimalware Software; Scanning and Removal Techniques; Schedule Scans and Run Updates; Create a System Restore Point; Educate the End User

Objectives covered
3 Software Troubleshooting
3.3 Given a scenario, use best practice procedures for malware removal
3.3.4 Remediate infected systems
3.3.4.1 Update antimalware software
3.3.4.2 Scanning and removal techniques (e.g., safe mode, preinstallation environment)
3.3.5 Schedule scans and run updates
3.3.6 Enable System Restore and create a restore point in Windows
3.3.7 Educate the end user

Domain 3:

Lesson 5

A+ (220-1102)

Mobile OS and App Issues – Part 1

Similar to desktop computers, mobile OS and apps have issues technicians need to know about so that these issues can be diagnosed and, if possible, solved without a mobile device needing to be sent back to its manufacturer for repair. Though a factory reset on a device can solve many issues, that action is usually unnecessary to solve common problems.

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 3
Topic: Common Mobile OS and App Issues
Subtopics: Application Fails to Launch; Application Fails to Close; Application Fails to Update; Slow to Respond; OS Fails to Update; Battery Life Issues; Random Reboots

Objectives covered
3 Software Troubleshooting
3.4 Given a scenario, troubleshoot common mobile OS and application issues
3.4.1 Common symptoms
3.4.1.1 Application fails to launch
3.4.1.2 Application fails to close/crashes
3.4.1.3 Application fails to update
3.4.1.4 Slow to respond
3.4.1.5 OS fails to update
3.4.1.6 Battery life issues
3.4.1.7 Randomly reboots

Purpose

After completing this and the next project, you will better understand mobile operating system and app issues.

Steps for Completion

1. What can be cleared in an app to help it launch if it consistently fails to launch?

   a. ________________

2. An app crashes frequently. What should be done with the app to attempt to mitigate the issue?

   a. ____

3. An app update fails multiple times. What should be done to try to get the app to update?

   a. ____

4. What could be low on a mobile device if an app has been slow to respond, even after an update?

   a. ______________________________________

5. What are three possible causes for a mobile OS failing to update when trying to update?

   a. _______________________________________

   b. ____

   c. ____

6. What are two mobile device settings than can affect battery life negatively?

   a. ____________________________

   b. ___________________________

7. What is a common software cause of random reboots?

   a. _______________________________________

Mobile OS and App Issues – Part 2

Many OS and app issues on mobile devices are connectivity-based issues. Network connectivity is easy to establish on mobile devices and just as easy to turn off on these devices. End users need to be aware of what can deactivate network connections on devices.

Purpose

Upon completing this project, you will better understand connectivity issues on mobile devices. You will need a smartphone or tablet to complete this project in full.

Steps for Completion

1. Which mode on a mobile device turns off all wireless communication?
   a. ________________________________
2. On a mobile device, ensure that the Autorotate, Bluetooth, and Wi-Fi settings are set to on.
3. What part of a smartphone could impede NFC's communication ability with another NFC-based device?
   a. ________________________________
4. What is the iOS equivalent of NFC?
   a. ________________________________
5. What is the default setting for people to communicate with using AirDrop?
   a. ________________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 3
Topic: Common Mobile OS and App Issues
Subtopics: Connectivity Issues; Screen does not Autorotate

Objectives covered
3 Software Troubleshooting
3.4 Given a scenario, troubleshoot common mobile OS and application issues
3.4.1 Common symptoms
3.4.1.8 Connectivity issues
3.4.1.8.1 Bluetooth
3.4.1.8.2 Wi-Fi
3.4.1.8.3 Near-field communication (NFC)
3.4.1.8.4 AirDrop
3.4.1.9 Screen does not autorotate

Domain 3:

Lesson 6

A+ (220-1102)

Mobile OS and App Security Concerns

Security concerns are not limited to desktop operating systems. Mobile operating systems and their apps have their own set of security concerns. One of the most important security apps for mobile devices is to ensure, as much as possible, that apps are only obtained from reputable sources. Each mobile operating system has a store containing apps that have been tested for legitimacy.

Purpose

Upon completing this project, you will better understand mobile operating system and app security concerns.

Steps for Completion

1. What is the file format for Android apps published to the Play Store?
    a. ______________________________
2. What is a legitimate exception to obtaining an Android app from the Play Store?
    a. ______________________________
    ____
3. An Android developer needs to stage GPS locations to test an app. In which mode should a device be for those tests?
    a. ______________________________
4. Indicate the OS to which each act applies:
    a. Root a device: ______________________________
    b. Jailbreak the device: ______________________________
5. What are two indicators that an app one wants to obtain could be a spoof of an app?
    a. ______________________________
    b. ______________________________
    ____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 3
Topic: Common Mobile OS and App Security Issues
Subtopics: APK Source; Developer Mode; Root Access/Jailbreak; Bootleg/Malicious App

Objectives covered
3 Software Troubleshooting
3.5 Given a scenario, troubleshoot common mobile OS and application security issues
3.5.1 Security concerns
3.5.1.1 Android package (APK) source
3.5.1.2 Developer mode
3.5.1.3 Root access/jailbreak
3.5.1.4 Bootleg/malicious application
3.5.1.4.1 Application spoofing

LearnKey

Mobile OS and App Security Issues

Some mobile OS and app security issues are similar to security issues found on desktops and desktop apps. Some issues may not seem security-related at first. Still, given the open nature of many mobile device network connections, mobile devices are susceptible to attacks, especially on personal data on those devices.

Purpose

Upon completing this project, you will better understand mobile OS and app security issues. NOTE: You will need a smartphone or tablet to complete this project in full.

Steps for Completion

1. On a mobile device, check the data usage for apps. Are any apps using an inordinately high amount of data?
   a. ____________________
2. Is the device at or near a data usage limit for a time period?
   a. ____________________
3. How much RAM and/or storage space is used on your device?
   a. ____________________
4. What is one main cause of a device having limited or no internet connectivity while a person is out in public with a mobile device?
   a. ____________________
5. A mobile device is experiencing a high number of ads and some fake security warnings. What should be done with the device?
   a. ____________________
6. An app is behaving erratically. What should be done first to the app?
   a. ____________________
   ____
7. What can help strengthen a mobile device against personal data being leaked from the device?
   a. ____________________

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 3

Topic: Common Mobile OS and App Security Issues

Subtopics: High Network Traffic; Sluggish Response Time; Data-Usage Limit Notification; Limited Internet Connectivity; No Internet Connectivity; High Number of Ads; Fake Security Warnings; Unexpected Application Behavior; Leaked Personal Files/Data

Objectives covered

3 Software Troubleshooting

3.5 Given a scenario, troubleshoot common mobile OS and application security issues

3.5.2 Common symptoms

3.5.2.1 High network traffic

3.5.2.2 Sluggish response time

3.5.2.3 Data-usage limit notification

3.5.2.4 Limited internet connectivity

3.5.2.5 No internet connectivity

3.5.2.6 High number of ads

3.5.2.7 Fake security warnings

3.5.2.8 Unexpected application behavior

3.5.2.9 Leaked personal files/data

Domain 4:
Lesson 1

A+ (220-1102)

Ticketing Systems

IT processes must be documented well to help people unfamiliar with them understand what to do. One common way of documenting processes is to use a ticketing system. User information, device information, problem descriptions, categorizing problems, severity, escalation levels, and clear communication are all critical considerations when using a ticketing system.

Purpose

Upon completing this project, you will better understand ticketing systems.

Steps for Completion

1. Determine whether each statement is true or false. Use T for true and F for false.

    a. _________ Some ticketing systems can pull user information from another data source.

    b. _________ Technicians need to know what device they are working on because different devices may have different solutions to problems.

    c. _________ A problem description is usually unnecessary unless the problem is complicated.

    d. _________ Choosing a category for a problem helps technicians understand the problem better by classifying it.

    e. _________ Technicians should not escalate problems unless they involve major security issues.

    f. _________ When fixing a simple problem, writing that the ticket is closed as the resolution is sufficient.

2. What is the purpose of a ticketing system?

    a. ____
    ____

3. Why should a severity level be included on a ticket?

    a. ____
    ____

4. What would be a good, descriptive closing for a ticket in which you reset someone's IP address?

    a. ____
    ____
    ______

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 4
Topic: Documentation Best Practices
Subtopics: User Information on Ticketing Systems; Device Information; Problem, Category, and Severity; Escalation Levels; Clear and Concise Communication

Objectives covered
4 Operational Procedures
4.1 Given a scenario, implement best practices associated with documentation and support systems information management
4.1.1 Ticketing systems
4.1.1.1 User information
4.1.1.2 Device information
4.1.1.3 Description of problems
4.1.1.4 Categories
4.1.1.5 Severity
4.1.1.6 Escalation levels
4.1.1.7 Clear, concise written communication

Asset Management

Asset management is a necessary consideration for larger businesses. When a business has multiple assets, the business must keep track of those assets. In addition, technicians should know how to manage assets at different points in their life cycles and know what warranties and licenses are active.

Purpose

Upon completing this project, you will better understand asset management.

Steps for Completion

1. What is the purpose of an inventory list?
   a. ______________________________
   ____

2. Why might a business with many assets use a database to track inventory rather than a spreadsheet?
   a. ______________________________
   ____
   ____

3. What are the two purposes of using asset tags or serial numbers?
   a. ______________________________
   ____
   ____

4. List the eight steps of the procurement life cycle from first to last.
   a. ______________________________
   ____
   ____
   ____
   ____

5. Why is it important to know if a device is still under warranty before working on it?
   a. ______________________________
   ____
   ____

6. Why should technicians know what licenses a business has?
   a. ______________________________
   ____
   ____

7. Who should assign users to devices?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 4
Topic: Documentation Best Practices
Subtopics: Inventory List; Database System; Asset Tags and IDs; Procurement Life Cycle; Warranty and Licensing; Assigned Users

Objectives covered
4 Operational Procedures
4.1 Given a scenario, implement best practices associated with documentation and support systems information management
4.1.2 Asset management
4.1.2.1 Inventory lists
4.1.2.2 Database system
4.1.2.3 Asset tags and IDs
4.1.2.4 Procurement life cycle
4.1.2.5 Warranty and licensing
4.1.2.6 Assigned users

Documents and Knowledge Bases

There are several types of documents technicians may come across as part of a business's IT environment. Some examples include acceptable use policies (AUPs), network topology diagrams, incident reports, standard operating procedures, new-user setup checklists, and end-user setup checklists. In addition, some businesses may have documents regarding regulatory compliance requirements to which certain businesses are subject.

Knowledge bases help technicians with troubleshooting. Knowledge bases contain information reported by users and other technicians that can help solve device and application-related problems.

Purpose

Upon completing this project, you will better understand documents for an IT environment and knowledge bases.

Steps for Completion

1. Match the document to its description.

   A. AUP
   B. Network topology diagram
   C. Incident report
   D. Standard operating procedure

   a. _________ A document that details how to complete processes within a business

   b. _________ A document that dictates what employees can and cannot do with equipment, email, and other company resources

   c. _________ A document that helps clarify and track events and their investigations

   d. _________ A document that shows the physical placement of devices in a network

2. Determine whether each statement is true or false. Use T for true and F for false.

   a. _________ A best practice is to ensure new employees read and sign a company's AUP after a month of employment.

   b. _________ New-user setup checklists should not be changed once they are implemented.

   c. _________ End-user termination checklists help ensure IT staff knows what equipment needs to be retrieved when an employee leaves a company.

3. In a web browser, navigate to https://support.microsoft.com/en-us

4. In the How can we help you field, search for **Windows 11** and browse through the available articles.

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 4
Topic: Documentation Best Practices
Subtopics: AUP; Network Topology Diagram; Regulatory Compliance Requirements; Incident Reports; Standard Operating Procedures; New User Setup Checklist; End User Termination Checklist; Knowledge Base/Articles

Objectives covered
4 Operational Procedures
4.1 Given a scenario, implement best practices associated with documentation and support systems information management
4.1.3 Types of documents
4.1.3.1 Acceptable use policy (AUP)
4.1.3.2 Network topology diagram
4.1.3.3 Regulatory compliance requirements
4.1.3.4 Incident reports
4.1.3.5 Standard operating procedures
4.1.3.6 New user setup checklist
4.1.3.7 End user termination checklist
4.1.4 Knowledge base/articles

Domain 4:

Lesson 2

A+ (220-1102)

LearnKey

Change Management

Change management is a system in which processes, equipment, and other changes in an IT infrastructure are approved and tracked. Having a change management process in place helps to implement changes smoothly with minimal impact on users.

Purpose

Upon completing this project, you will better understand rollback plans, sandbox testing, and responsible staff members.

Steps for Completion

1. Any attempted ____________________ needs a rollback plan.
2. When should a rollback plan be used?
    a. ____
    ____
3. What is sandbox testing?
    a. ____
    ____
4. What is the purpose of sandbox testing?
    a. ____
    ____
5. Who is likely to be designated a responsible staff member for a change?
    a. ____
    ____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
Topic: Change Management Best Practices
Subtopics: Rollback Plan; Sandbox Testing and Responsible Staff

Objectives covered
4 Operational Procedures
4.2 Explain basic change-management best practices
4.2.1 Documented business processes
4.2.1.1 Rollback plan
4.2.1.2 Sandbox testing
4.2.1.3 Responsible staff member

Change Request Forms

Change request forms are necessary to manage a business's IT environment. Technicians must follow a process for changes, beginning with a change request form. Using change request forms helps ensure minimal disruption to a business's day-to-day tasks.

Purpose

Upon completing this project, you will better understand change request forms.

Steps for Completion

1. The ____________________ management process should start with a change request form.
2. What two pieces of information should be included when describing the reason for a change on a request form?
   a. ____
   ____
3. What should technicians consider when choosing a date and time for a change to take place?
   a. ____
   ____
   ____
4. Describe two ways a business would be impacted by upgrading the IT infrastructure to Windows 11.
   a. ____
   ____
   ____
   ____
   ____
   ____
5. It is important that risks associated with a change be well-defined, as a request form without a risk __________________________ is likely to be rejected.
6. Why is a change board necessary for the change management process?
   a. ____
   ____
   ____
7. How should technicians help end users accept a change?
   a. ____
   ____

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 4
Topic: Change Management Best Practices
Subtopics: Request Forms; Purpose and Scope of Change; Time and Impact of Change; Risk Analysis; Change Board Approvals; End-User Acceptance

Objectives covered
4 Operational Procedures
4.2 Explain basic change-management best practices
4.2.2 Change management
4.2.2.1 Request forms
4.2.2.2 Purpose of the change
4.2.2.3 Scope of the change
4.2.2.4 Date and time of the change
4.2.2.5 Affected systems/impact
4.2.2.6 Risk analysis
4.2.2.7 Change board approvals
4.2.2.8 End-user acceptance

Backups

Technicians should back up important data on all devices regularly. Backups can be saved to hardware or devices such as hard drives, but in many cases, backups are saved to the cloud. Types of backups include full, incremental, differential, and synthetic backups. When performing backups, technicians must also consider the frequency in which they should test backups and where the backups will be stored.

Purpose

Upon completing this project, you will better understand backups.

Steps for Completion

1. What is a full backup?
   a. ______________________________
   ____
2. What is an incremental backup?
   a. ______________________________
   ____
   ____
3. What is a differential backup?
   a. ______________________________
   ____
4. What is a synthetic backup?
   a. ______________________________
   ____
   ____
5. How frequently should backups be tested?
   a. ______________________________
6. What is the minimum number of copies of data technicians must store off-site for backups to be considered safe? ____________
7. Describe the 3-2-1 backup rule.
   a. ______________________________
   ____
   ____
8. Describe the Grandfather-Father-Son (GFS) backup rotation scheme.
   a. ______________________________
   ____
   ____

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 4
Topic: Backup and Recovery
Subtopics: Full; Incremental; Differential; Synthetic; Backup Testing; Onsite vs. Offsite and 3-2-1; GFS

Objectives covered
4 Operational Procedures
4.3 Given a scenario, implement workstation backup and recovery methods
4.3.1 Backup and recovery
4.3.1.1 Full
4.3.1.2 Incremental
4.3.1.3 Differential
4.3.1.4 Synthetic
4.3.2 Backup testing
4.3.3 Backup rotation schemes
4.3.3.1 On-site vs. off-site
4.3.3.2 Grandfather-Father-Son (GFS)
4.3.3.3 3-2-1 backup rule

Domain 4:

Lesson 3

A+ (220-1102)

LearnKey

Common Safety Procedures

There are some common safety procedures to follow when working on equipment. Technicians should use items such as an electrostatic discharge (ESD) strap or ESD mat to avoid static discharge inside a device. In addition, it is important to ground the equipment on which one works to prevent a short circuit.

Another common safety procedure involves working on power supplies and monitors. The best practice with power supplies and monitors is to replace, not repair, them because they present an electrocution risk. Technicians can work on most components as long as they handle them correctly. It is also essential to comply with government regulations when handling components, especially regarding their disposal.

Purpose

Upon completing this project, you will become more familiar with common safety procedures.

Steps for Completion

1. Why is it important to prevent the transfer of static electricity to computer components?
   a. ______________________________
   ____
2. Why does computer equipment need to be properly grounded?
   a. ______________________________
   ____
   ____
3. List and describe the three types of equipment grounding:
   a. ______________________________
   b. ______________________________
   c. ______________________________
4. Why should one never place their hands inside a plugged-in printer?
   a. ______________________________
5. What should one use to store hardware components not installed on a computer?
   a. ______________________________
6. Label the following statement as true or false.
   a. ____________ Component handling should comply with government regulations, beginning at the local level and applying federal and state regulations.

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 4

Topic: Common Safety Procedures

Subtopics: ESD Straps; ESD Mats; Equipment Grounding; Proper Power Handling; Components and Antistatic Bags; Compliance with Government Regulations

Objectives covered

4 Operational Procedures

4.4 Given a scenario, use common safety procedures

4.4.1 Electrostatic discharge (ESD) straps

4.4.2 ESD mats

4.4.3 Equipment grounding

4.4.4 Proper power handling

4.4.5 Proper component handling and storage

4.4.6 Antistatic bags

4.4.7 Compliance with government regulations

LearnKey

Personal Safety Procedures

Equally important to protecting computer equipment is protecting the technician working on it. The first personal safety procedure is unplugging a computer before repairing it. Unplugging a PC stops most electrical current from flowing through it and reduces the risk of electrical issues.

Another personal safety procedure is using proper lifting techniques to avoid back injury. When picking up heavy equipment, a person should let their legs lift an item and avoid twisting while lifting.

Sometimes, computer equipment rooms can catch fire; thus, a fire extinguisher should be present within a building as part of electrical fire safety. Everyone in a building containing this extinguisher should know its location and how to use it. Other personal safety equipment includes safety goggles and an air filtration mask.

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 4
Topic: Common Safety Procedures
Subtopics: Disconnect Power Before Repairing; Lifting Techniques, Fire Safety; Protecting the Eyes, Nose, and Mouth

Objectives covered

4 Operational Procedures
4.4 Given a scenario, use common safety procedures
4.4.8 Personal safety
4.4.8.1 Disconnect power before repairing PC
4.4.8.2 Lifting techniques
4.4.8.3 Electrical fire safety
4.4.8.4 Safety goggles
4.4.8.5 Air filtration mask

Purpose

Upon completing this project, you will become more familiar with personal safety procedures.

Steps for Completion

1. Unplugging a PC will not stop the flow of electrical current in which component?
    a. ______________________________
    ____
2. When transporting heavy equipment, what tool can help carry these items?
    a. ______________________________
3. What class of fire extinguishers should be present within a building as part of electrical fire safety?
    a. ______________________________
4. Who should know how to use a fire extinguisher in a building containing computer equipment?
    a. ______________________________
5. What is the main objective of both safety goggles and an air filtration mask?
    a. ______________________________
    ____

LearnKey

Environmental Impacts

A business's failure to comply with local and state environmental laws can lead to heavy fines, especially regarding asset disposal. Thus, following local and state environmental laws is more important than any other guidance received here.

A Material Safety Data Sheet (MSDS) shows the proper handling and disposal of a component containing hazardous material, such as a battery or a toner cartridge. An MSDS guides users on what to do if this hazardous material comes in contact with a human or is released when it is not supposed to be.

When disposing of a laptop battery or toner cartridges, users should research the policy for their area. Regulations for the disposal of other devices and assets vary by state. One should research how to dispose of electronic waste on sites such as the Environmental Protection Agency (EPA) website.

Purpose

Upon completing this project, you will better understand the environmental impacts of computer equipment disposal.

Steps for Completion

1. What is a typical guideline for disposing of a laptop battery?
   a. ______________________________
2. Where can toner cartridges often be taken for disposal or recycling?
   a. ______________________________
   ____
3. Label the following statement as true or false.
   a. ______________ Most places legally allow printer toner to be thrown out with the garbage.
4. What is the overarching theme for the disposal of other computer equipment through stores and resellers?
   a. ______________________________
   ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 4

Topic: Environmental Impacts and Controls

Subtopics: Proper Battery Disposal; Proper Toner Disposal; Proper Disposal of Other Devices

Objectives covered

4 Operational Procedures

4.5 Summarize environmental impacts and local environmental controls

4.5.1 Material safety data sheet (MSDS)/documentation for handling and disposal

4.5.1.1 Proper battery disposal

4.5.1.2 Proper toner disposal

4.5.1.3 Proper disposal of other devices and assets

LearnKey

Local Environmental Controls

Local environmental controls include temperature, humidity, ventilation, and dust. Ventilation should be prevalent throughout a building, but a server room environment is the most critical area to monitor. Many high-powered, heat-generating computers are close to each other in a server room. Thus, servers should be set up in a well-ventilated area with a controlled temperature to prevent overheating. Dust is a conduit for heat and electricity and should be removed from computer components when found.

Purpose

Upon completing this project, you will become more familiar with local environmental controls.

Steps for Completion

1. What are the ideal temperature range and humidity level for a server room?
   a. ______________________________
   ____
   ____
2. What happens in an environment that is too humid for computers?
   a. ______________________________
   ____
3. Label the following statement as true or false.
   a. ____________ Ventilation needs to pull cold air away from equipment and push hot air into equipment.
4. What may happen if dust is left inside a computer for too long?
   a. ______________________________
5. List two tools for removing dust from inside a computer:
   a. ______________________________
   b. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
Topic: Environmental Impacts and Controls
Subtopics: Equipment Location and Placement; Dust, Compressed Air, and Vacuums

Objectives covered
4 Operational Procedures
4.5 Summarize environmental impacts and local environmental controls
4.5.2 Temperature, humidity-level awareness, and proper ventilation
4.5.2.1 Location/equipment placement
4.5.2.2 Dust cleanup
4.5.2.3 Compressed air/vacuums

Power Surges and Failures

Sometimes, power issues can cause data corruption on servers and other important devices. An Uninterruptable Power Supply (UPS) is a battery-powered backup for a business. A UPS keeps devices up and running for several minutes after a power outage; however, it is not a long-term power solution.

A surge suppressor helps protect devices from surges or unexpected spikes in voltage. While surges and spikes are over-voltage conditions, sags and brownouts are under-voltage. Sags are short dips, whereas brownouts are protracted drops in voltage.

Purpose

Upon completing this project, you will become more familiar with power surges and failures.

Steps for Completion

1. During a power outage, what does a UPS allow technicians to do?
   a. ____
   ____
   ____
2. If a hurricane strikes and power is out for days, what might one use to keep power up and running?
   a. ____
3. Which power issue rarely causes damage to electrical components?
   a. ____
   ____
4. Label the following statement as true or false.
   a. __________ A power strip provides the same protection for devices as a surge protector.
5. What tool helps protect equipment against sags and brownouts?
   a. ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 4

Topic: Environmental Impacts and Controls

Subtopics: Battery Backup; Surge Suppressor

Objectives covered

4 Operational Procedures

4.5 Summarize environmental impacts and local environmental controls

4.5.3 Power surges, under-voltage events, and power failures

4.5.3.1 Battery backup

4.5.3.2 Surge suppressor

Domain 4:

Lesson 4

A+ (220-1102)

Incident Response

Evidence must be gathered and held appropriately when a potential security incident occurs. Chain of custody is a chronological documentation of evidence, including how it was handled, when, and by whom. Once evidence is gathered, one should inform management immediately if there is a security breach. Equally important is preserving the hard drives containing an incident. One should also keep solid records of any incident to prevent future reoccurrences.

Purpose

Upon completing this project, you will better understand incident response procedures.

Steps for Completion

1. Why is it important to follow a chain of custody?
   a. ____
   ____
   ____
2. When should an incident be reported to law enforcement?
   a. ____
   ____
3. How does one tell if an encrypted hard drive, collected as evidence, is altered in any way?
   a. ____
   ____
   ____
4. What may happen in court if a hard drive is altered?
   a. ____
   ____
5. Label the following statement as true or false.
   a. ______________ Companies use comprehensive documentation to strengthen a company's IT security posture.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
Topic: Content, Licensing, and Policies
Subtopics: Chain of Custody; Inform Authorities; Hard Drive Integrity; Incident Documentation

Objectives covered
4 Operational Procedures
4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts
4.6.1 Incident response
4.6.1.1 Chain of custody
4.6.1.2 Inform management/law enforcement as necessary
4.6.1.3 Copy of drive (data integrity and preservation)
4.6.1.4 Documentation of incident

Licensing

Ensuring proper licensing for all software used within a company is part of managing an IT infrastructure. Valid licenses ensure that someone is not using software illegally because businesses risk heavy fines from the software vendor or a regulatory body. There are a few different types of valid licenses available for use. An end-user license agreement (EULA) defines what a customer may do with a software license.

Purpose

Upon completing this project, you will become more familiar with licensing.

Steps for Completion

1. What is an example of a license being valid through its software cycle?
   a. ______________________________
   ____
2. Which software license allows media files to be used only on authorized devices?
   a. ______________________________
3. What is a perpetual license?
   a. ______________________________
4. How does software become vulnerable when it is no longer supported?
   a. ______________________________
   ____
5. What distinction do some apps make between a personal use license and a corporate license?
   a. ______________________________
   ____
6. Open-source licenses are free and make what else available to users?
   a. ______________________________
   ____
7. Name a popular open-source suite that runs on multiple operating systems.
   a. ______________________________
8. Label the following statement as true or false.
   a. ______________________________ All free software is open-source software.

Project Details

Project file

N/A

Estimated completion time

10 minutes

Video reference

Domain 4

Topic: Content, Licensing, and Policies

Subtopics: Valid and Non-Expired Licenses; Personal Use vs. Corporate Licenses; Open-Source Licenses

Objectives covered

4 Operational Procedures

4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts

4.6.2 Licensing/digital rights management (DRM)/end-user license agreement (EULA)

4.6.2.1 Valid licenses

4.6.2.2 Non-expired licenses

4.6.2.3 Personal use license vs. corporate use license

4.6.2.4 Open-source license

Regulated Data

Regulated data is information that needs to be kept secure and confidential. Payment card data is regulated and falls under the Payment Card Industry Data Security Standard (PCI DSS). Banks and creditors enforce PCI DSS, not government entities. Other forms of data that must be kept secure and confidential include government-issued information and healthcare data. Data retention requirements define rules for storing these types of regulated data.

Purpose

Upon completing this project, you will better understand regulated data.

Steps for Completion

1. What is the Payment Card Industry Data Security Standard (PCI DSS)?
   a. ______________________________
2. What may happen to a company that does not adhere to PCI DSS?
   a. ______________________________
3. Give an example of personal, government-issued information.
   a. ______________________________
4. What is Personally Identifiable Information (PII)?
   a. ______________________________
5. How might the leaking of health data be detrimental to an employee?
   a. ______________________________
6. What is the principle of data retention?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
Topic: Content, Licensing, and Policies
Subtopics: Credit Card Transactions; Government Issued and PII; Healthcare Data; Data Retention Requirements

Objectives covered
4 Operational Procedures
4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts
4.6.3 Regulated data
4.6.3.1 Credit card transactions
4.6.3.2 Personal government-issued information
4.6.3.3 PII
4.6.3.4 Healthcare data
4.6.3.5 Data retention requirements

LearnKey

Professionalism

Computer technicians should use proper communication and professionalism in a business environment. Professionalism has several aspects, including attire, language, listening skills, attitude, and punctuality.

There are several ways to avoid appearing unprofessional in a business environment. Technicians should not show up for work in a t-shirt, ripped jeans, or flip-flops, as that is considered unprofessional. Technicians should avoid making customers feel inept with computers when speaking to them.

Technicians should always try to be on time for an appointment. Punctuality is one of the most important aspects of customer service in any field, including technical support.

Purpose

Upon completing this project, you will become more familiar with professionalism.

Steps for Completion

1. List the two forms of professional attire identified by CompTIA:
   a. ______________________________
   b. ______________________________
2. What type of language should technicians avoid when speaking to clients?
   a. ______________________________
   ____
3. What should a technician project when attempting to solve a customer's problem?
   a. ______________________________
4. When a customer explains a problem, what aspect of communication should a technician utilize?
   a. ______________________________
5. What does it mean to be culturally sensitive?
   a. ______________________________
   ____
   ____
6. Label the following statement as true or false.
   a. ____________ Technicians should use people's professional titles as a sign of respect.
7. If a technician cannot avoid being late to an appointment, what should they do?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
Topic: Communication and Professionalism
Subtopics: Professional Appearance and Attire; Proper Language; Positive Attitude and Confidence; Listen and Take Notes; Cultural Sensitivity; Punctuality

Objectives covered
4 Operational Procedures
4.7 Given a scenario, use proper communication techniques and professionalism
4.7.1 Professional appearance and attire
4.7.1.1 Match the required attire of the given environment
4.7.1.1.1 Formal
4.7.1.1.2 Business casual
4.7.2 Use proper language and avoid jargon, acronyms, and slang, when applicable
4.7.3 Maintain a positive attitude/project confidence
4.7.4 Actively listen, take notes, and avoid interrupting the customer
4.7.5 Be culturally sensitive
4.7.5.1 Use appropriate professional titles, when applicable
4.7.6 Be on time (if late, contact the customer)

Distractions and Difficult Customers

Another aspect of professionalism is avoiding distractions while working on customer issues. Customers want to ensure their money is paying for technical support, not a technician tending to personal matters. Every technician must deal with a difficult customer or situation at some point. Remaining calm and professional while handling this kind of situation is crucial. One should also avoid dismissing customer problems and being judgmental. Instead, one should actively listen and respond appropriately to clarify a customer's issue. Once a technician finishes helping a demanding customer, they must never disclose the experience via social media outlets.

Purpose

Upon completing this project, you will become familiar with avoiding different distractions and handling difficult customers.

Steps for Completion

1. What are two types of distractions a technician should avoid?
   a. ______________________________
2. Why should a technician avoid arguing with a customer?
   a. ______________________________
3. What is the danger in dismissing a customer problem and being judgmental?
   a. ______________________________
4. How can a technician verify to a customer that they understand a problem?
   a. ______________________________
5. Why should technicians never disclose a challenging customer experience via social media?
   a. ______________________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 4
Topic: Communication and Professionalism
Subtopics: Avoid Distractions; Avoid Arguments; Customer Problems and Judgment; Clarify Customer Statements; Social Media Disclosure Avoidance

Objectives covered

4 Operational Procedures
4.7 Given a scenario, use proper communication techniques and professionalism
4.7.7 Avoid distractions
4.7.7.1 Personal calls
4.7.7.2 Texting/social media sites
4.7.7.3 Personal interruptions
4.7.8 Dealing with difficult customers or situations
4.7.8.1 Do not argue with customers or be defensive
4.7.8.2 Avoid dismissing customer problems
4.7.8.3 Avoid being judgmental
4.7.8.4 Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding)
4.7.8.5 Do not disclose experience via social media outlets

LearnKey

Meeting Customer Expectations

Communication and professionalism also involve dealing appropriately with a customer's private materials. Additionally, technicians should try to meet customer expectations, control these expectations when necessary, create an agreeable timeline for work completion, and communicate the status of solving a customer's problem.

When working at a customer site, technicians should try not to see confidential information. Often businesses require people to sign a non-disclosure agreement (NDA) to ensure they do not expose personal information outside a company.

Part of setting and meeting customer expectations is providing proper documentation on services rendered. This documentation should include the services provided for repair, installation, or similar services. Later, a technician may call a customer to verify satisfaction with the job done.

Purpose

Upon completing this project, you will better understand meeting customer expectations.

Steps for Completion

1. What should one tell a customer who asks to have their old computer made ready for something as sophisticated as virtual reality (VR)?
   a. ______________________________
   ____
2. What is the purpose of documenting work a technician has performed?
   a. ______________________________
   ____
3. What can follow-up calls help a business do?
   a. ______________________________
   ____
   ____
4. Where might a technician see confidential material within a company?
   a. ______________________________
   ____
5. If a technician signs an NDA and does not share confidential information, why does it matter if they see it?
   a. ______________________________
   ____

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 4

Topic: Communication and Professionalism

Subtopics: Offer Repair/Replacement Options; Provide Documentation for Services; Follow Up with Customer; Deal with Confidential Material

Objectives covered

4 Operational Procedures

4.7 Given a scenario, use proper communication techniques and professionalism

4.7.9 Set and meet expectations/timeline and communicate status with the customer

4.7.9.1 Offer repair/replacement options, as needed

4.7.9.2 Provide proper documentation on the services provided

4.7.9.3 Follow up with customer/user at a later date to verify satisfaction

4.7.10 Deal appropriately with customers' confidential and private materials

4.7.10.1 Located on a computer, desktop, printer, etc.

Domain 4:

Lesson 5

A+ (220-1102)

LearnKey

Script File Types

Script files are used to automate administrative processes for both devices and networks. Technicians do not need to be full-fledged programmers, but they do need to look at a script and know the overall reason for a script in a given situation.

Furthermore, technicians need to know what type of script to use, given the situation. For example, if a networking device is already controlled using Python scripts, then any further scripts should be written using Python.

Purpose

Upon completing this project, you will better understand script file types and their uses.

Steps for Completion

1. Which script file type has commands that can be run in a command-line environment?

    a. ______________________________

2. Which script file types use cmdlets to perform tasks on devices, user accounts, and other computing aspects?

    a. ______________________________

3. Name a script file type that requires an engine to run its scripts:

    a. ______________________________

4. Which type of script file is often used to enhance a webpage?

    a. ______________________________

5. Which script file type runs commands on Linux devices?

    a. ______________________________

6. What is one advantage .vbs files have over .bat files?

    a. .______________________________

Project Details

Project file

N/A

Estimated completion time

5 minutes

Video reference

Domain 4

Topic: Scripting Basics

Subtopics: Batch Files; PowerShell Files; Visual Basic Script Files; Shell Files; JavaScript Files; Python Files

Objectives covered

4 Operational Procedures

4.8 Identify the basics of scripting

4.8.1 Script file types

4.8.1.1 .bat

4.8.1.2 .ps1

4.8.1.3 .vbs

4.8.1.4 .sh

4.8.1.5 .js

4.8.1.6 .py

Use Cases for Scripting

For scripting to be effective, one must know the best use cases for using script files. For example, a one-time configuration process probably does not require a script, though in some cases, as with Azure deployments, a script can be generated and then used to deploy a similar resource the next time one is needed.

Purpose

Upon completing this project, you will better understand use cases for scripting.

Steps for Completion

1. What is the command-line command for automating a shutdown, with a restart, on a machine named test1?
    a. ______________________________
2. What should be done with a drive mapping to point to an installation file in a script when the mapping is no longer needed?
    a. ______________________________
3. What line of script can be used to automate the backup of the Users folder on drive C to the Backup folder on drive E and have the backup include empty folders?
    a. ______________________________
4. Which symbol writes a command-line output to a text file?
    a. ______________________________
5. Which PowerShell cmdlet adds a package of cmdlets that can be used to do specific configuration tasks on a device?
    a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
Topic: Scripting Basics
Subtopics: Automation and Restarts; Network Drives and Installs; Automated Backups; Information Gathering; Initiating Updates

Objectives covered
4 Operational Procedures
4.8 Identify the basics of scripting
4.8.2 Use cases for scripting
4.8.2.1 Basic automation
4.8.2.2 Restarting machines
4.8.2.3 Remapping network drives
4.8.2.4 Installation of applications
4.8.2.5 Automated backups
4.8.2.6 Gathering of information/data
4.8.2.7 Initiating updates

Script Usage Considerations

Though scripts help save time by automating tasks, performing installs, gathering information, and initiating updates, scripts can cause inherent problems for systems and network infrastructure. Technicians need to be aware of these problems and look over scripts to ensure they possess little to no risk for a system before running them.

Purpose

Upon completing this project, you will better understand script usage considerations and how to ensure scripts do not damage a system or infrastructure.

Steps for Completion

1. Which add-ons and modules are safe to add to scripting platforms?
   a. ______________________________
2. What is the PowerShell cmdlet for installing a module?
   a. ______________
3. Which command makes changes to a system registry?
   a. _______
4. What can cause the wrong folders to be updated using command-line commands such as copy, xcopy, robocopy, or setx?
   a. __________________________________
5. What do endless loops in scripts cause?
   a. _____________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
Topic: Scripting Basics
Subtopics: Unintentionally Introducing Malware; Inadvertent System Settings Changes; Resource Mishandling

Objectives covered
4 Operational Procedures
4.8 Identify the basics of scripting
4.8.3 Other considerations when using scripts
4.8.3.1 Unintentionally introducing malware
4.8.3.2 Inadvertently changing system settings
4.8.3.3 Browser or system crashes due to mishandling of resources

Remote Access Technologies

Remote access, when used properly, can save lots of time and effort on user support as technicians can perform tasks on devices without physically being at these devices. Operating systems in place and available technologies in a home or business will dictate the type of remote access technologies available to support these devices.

Some remote access technologies allow the recipient of support to see what is being done to a device, while some do not.

Purpose

Upon completing this project, you will better understand the differences among popular remote access technologies.

Steps for Completion

1. On which port does RDP run?
   a. ______________________________
2. Which edition of Windows does not support RDP?
   a. ______________________________
3. A remote worker needs a secure connection to a corporate office for transferring data. What should the remote worker use?
   a. ______________________________
4. What is an alternative to RDP that is open source and runs on port 5900?
   a. ______________________________
5. Which remote access method is often used to connect one to Linux devices and is a secure alternative to FTP?
   a. ______________________________
6. The Identity Secure Score within Azure is an example of which type of remote technology?
   a. ______________________________
7. Which remote access method should be used if a person wants help on a device and wants to see what a technician is doing on the screen while working on the device?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
Topic: Remote Access Technologies
Subtopics: RDP; VPN; VNC; SSH; RMM; MSRA

Objectives covered
4 Operational Procedures
4.9 Given a scenario, use remote access technologies
4.9.1 Methods/tools
4.9.1.1 RDP
4.9.1.2 VPN
4.9.1.3 Virtual network computer (VNC)
4.9.1.4 Secure Shell (SSH)
4.9.1.5 Remote monitoring and management (RMM)
4.9.1.6 Microsoft Remote Assistance (MSRA)

LearnKey

Third-Party Tools for Remote Access

With the advent of remote work and online meetings, businesses have turned more to using third-party remote access tools for tasks such as meetings, conferences, and collaboration. Technicians need to know how to support these tools and be educated enough in these tools to give recommendations to businesses based on needs and security requirements.

Purpose

Upon completing this project, you will better understand third-party tools and their uses in remote access.

Steps for Completion

1. Name two tools that can be classified as screen-sharing software:
   a. ______________________________
   ____
2. Name three tools that can be classified as video-conferencing software:
   a. ______________________________
   ____
3. What is one important security aspect of file transfer software?
   a. ______________________________
   ____
4. What is the main purpose of desktop management software?
   a. ______________________________
   ____
5. Why should one use Secure Shell over Telnet for data transfers?
   a. ______________________________

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
Topic: Remote Access Technologies
Subtopics: Third-Party Tools; Security Considerations

Objectives covered
4 Operational Procedures
4.9 Given a scenario, use remote access technologies
4.9.1 Methods/tools
4.9.1.7 Third-party tools
4.9.1.7.1 Screen-sharing software
4.9.1.7.2 Video-conferencing software
4.9.1.7.3 File transfer software
4.9.1.7.4 Desktop management software
4.9.2 Security considerations of each access method

Appendix

A+ (220-1102)

Glossary

Term	Definition
.app	An extension on some apps that contain executables to files within macOS.
.bat	The extension for batch files, which are files that carry tasks that can be performed in a command-line environment.
.dmg	A file type that is a basic installation file within macOS.
.js	The extension for JavaScript files, which are files mainly used to enhance content on webpages.
.pkg	A file type for macOS that is a basic installation file with a wizard that guides a person through an installation.
.ps1	The extension for PowerShell scripts, which are scripts that run verb-noun cmdlets, which perform administrative tasks on devices.
.py	The extension for Python files. Python is a very versatile programming language used to build apps and process automation scripts.
.sh	The extension for shell scripts, which are files used to run commands on Linux devices.
.vbs	The extension for Visual Basic scripts, which are programming scripts used to automate processes on devices.
3-2-1 Backup Rule	A backup rule which states that three copies of data are kept at all times, with two copies on-site and one copy off-site.
Access Control Vestibule	A room between two security doors used to verify that everyone entering the first security door is authorized and has permission to enter the second security door.
Accounts	A settings area that allows for creating and managing user accounts on a device.
ACL	An Access Control List (ACL) is a list that defines the people and groups that have access to a resource and the specific access they have to that resource.
Active Directory	A centralized, client-server system in which user accounts, groups, attributes, and rights are centrally managed within a domain.
Ad Blocker	A tool that blocks unwanted advertisements that appear on webpages.
Administrative Tools	A group of tools used to provide information on a device and allow configuration changes on a device.
Administrator Account	A Windows account that has complete control of a device.
AES	Advanced Encryption Standard (AES) is an encryption standard that can encrypt data using up to 256-bit encryption for strong data protection.
Air Filtration Mask	A mask worn to help keep dust particles and chemicals away from one's nose and mouth.
AirDrop	An Apple-based connections service that allows devices in close proximity to one another to share information with each other.
Alarm System	A system used to deter unauthorized entry into a building or secure area of a building.
Android	A mobile device operating system, based off Linux, and found on many different brands of tablets and smartphones.
Antimalware	Software used to eradicate malware on devices.
Antistatic Bag	A bag that has mechanisms in place to help prevent devices such as network cards, hard drives, and other peripherals from receiving static electricity.
APFS	Apple File System (APFS) is found on Macs and supports encryption, compression, and snapshots on solid-state drives.
APK	An Android Package (APK) file is an app package distributed in the Play Store and through third-party sites.

Term	Definition
Apple ID	A username used to obtain apps from the App Store for Apple devices and can help one synchronize data across Apple devices.
Application Spoofing	A malicious app pretending to be a legitimate app.
Apps	In the context of settings, an area to where one can control how apps are installed on a device.
apt-get	A Linux command, used on some versions of Linux, which runs installation packages on devices.
Asset Tag	A label used to identify an asset within a business.
Attribute	In the context of files and folders, a characteristic of a file or folder, such as the file or folder being read-only or ready to be archived.
AUP	An Acceptable Use Policy (AUP) is a document that outlines what employees can and cannot do with equipment, email, and other company resources.
Authenticator App	An app used to confirm sign-in requests to other apps and systems.
AutoPlay	A file that controls the ability to automatically start media when that media is entered into a device.
AutoRun	A file used to automatically start installation files on removable media.
Badge Reader	A device that reads smart cards and authenticates people to secure areas of a building.
Bash	A popular shell used in Linux for running command-line commands within Linux.
Biometrics	The act of using something about a person as an authentication mechanism.
BIOS	The Basic Input Output System (BIOS) is a tool that controls hardware and other system settings and runs independently of an operating system.
BIOS Password	A password set that must be entered before a system can boot into its operating system.
BitLocker	A Windows feature that encrypts an entire hard drive.
BitLocker To Go	A version of BitLocker that encrypts external hard drives.
Bluetooth	A networking protocol in which devices, usually 30 feet apart or less, pair up with each other and communicate with each other.
Bollard	A thick vertical post used to prevent vehicles from entering an area.
Boot Sector Virus	A virus that infects the master boot record of an operating system and can, in turn, infect an entire operating system.
Botnet	A network of computers used for carrying out DDoS attacks.
Browser Data Synchronization	The synchronizing of browser history, settings, and bookmarks across devices tied to a user account.
Brute-Force Attack	An attack in which repeated attempts are made to crack a password until it is cracked.
BSOD	The Blue Screen of Death (BSOD) is a blue screen that appears when a system crashes, displays an error message, and eventually restarts.
BYOD	Bring Your Own Device (BYOD) is a category of personal devices that are used on corporate networks, usually through setting policies that determine the criteria for personal devices being allowed on corporate networks.
C Class	A class needed for a fire extinguisher in a place with computer equipment as a C Class fire extinguisher puts out electrical fires.
Cable Lock	A lock used to lock laptops to a desk and deter people from stealing the laptop.
Cache	In the context of webpages, saved information on webpages that loads when a webpage is requested so that the content of a webpage does not need to be downloaded each time it is requested.
cat	A Linux command that shows the contents of a file.
cd	A command-line command that changes the directory of focus for a person.

Term	Definition
Certificate Manager	A tool used to manage user and device-based certificates on a device.
Certificate of Destruction	A document that verifies that documents and hard drives meant for destruction have been destroyed properly.
Chain of Custody	A form of evidence handling in which every piece of evidence needs to be documented, timestamped, and tracked to be admissible in a court of law.
Change Management	A cycle in which changes are proposed, justified, and, if approved, carried out with a rollback plan in case the change does not work as intended.
Channel	In the context of wireless networks, a range within a frequency on which devices can communicate with each other.
chkdsk	A command-line command that attempts to fix disk errors.
chmod	A Linux command that changes permission on a file or folder.
chown	A Linux command that changes the ownership on a file or folder.
Chrome OS	A browser-based, cloud storage-driven operating system used on Chromebooks.
Cipher Lock	A lock that requires a combination to be entered before the lock will unlock.
Clean Install	A Windows installation that does not carry over any settings or files from a previous Windows installation.
Compatibility Mode	A mode in which an app runs as if it were on an older operating system.
Content Filtering	A setting that helps block unwanted content from a device or a network.
copy	A command-line command that copies files from one location to another.
Corporate License	A paid license for software that typically has few, if any restrictions on how the software can be used.
cp	A Linux command that copies a file from one folder to another.
Cryptominer	A takeover of a machine to where the machine's processor is used to solve intense mathematical puzzles to receive Bitcoin. This takeover slows down a device tremendously.
Data-At-Rest Encryption	The encryption of data while it is being stored on a device and not being transmitted to other devices.
Database System	An app that hosts a database and its tables, views, and programmed objects.
DDoS	A Distributed Denial of Service (DDoS) attack is a DoS attack that uses a network of multiple computers to carry out DoS attacks.
Default Gateway	A router that connects a LAN to the internet.
Definition Files	Files that have fixes against known malware and are used to eradicate malware from a device.
Degaussing	The act of taking a specifically designed electromagnet to a hard drive, with the idea that a magnetic field is applied to the drive, which wipes out data on the drive.
Developer Mode	A mode on Android in which developers have options such as fake GPS locations and other administrative tools to use while developing apps.
Device Manager	A list of hardware within and attached to devices that shows the status of each hardware piece and provides a means by which hardware drivers can be updated.
Devices	A settings area that allows for adding and managing Bluetooth and similar devices and printers to a computer.
Devices and Printers	A tool that allows one to install, share, and manage printers and similar devices locally or on a network.
df	A Linux command that shows the disk partitions on a device and the free space on each partition.
DHCP Reservation	An IP address, within a DHCP pool, which is reserved for a specific MAC address and prevents a device from needing a static IP address.
Dictionary Attack	An attack in which dictionary words are used to attempt to crack a password.

Term	Definition
Differential Backup	A backup that backs up data changed since the most recent full backup.
dig	A Linux command that obtains DNS server information from a current device or a specific domain.
dir	A command-line command that lists the contents of a directory.
Disk Cleanup	A tool that lists the size of and gives a person an option to remove temporary files, downloaded program files, and Recycle Bin files from a device.
Disk Defragmenter	A tool that brings together file fragments on magnetic hard drives.
Disk Management	A tool used to display, format, and partition hard drives on a system.
Disk Utility	A macOS feature that shows the amount of space remaining on a hard drive, the capacity of the drive, and other pertinent drive information.
diskpart	An interactive command-line command that shows DNS information on a device or, if desired, a different device.
Displays	On macOS, a window that allows one to configure multiple displays and their resolutions.
DNS	Domain Name Server (DNS) is a service that resolves hostnames to IP addresses.
Dock	A toolbar in macOS that allows one to organize and easily access commonly used apps, files, and folders.
Domain	A client-server network where one or more central servers store user accounts and their attributes.
DoS	A Denial of Service (DoS) attack is an attempt to flood a network with useless data and disrupt or halt the production ability of a network and its devices.
DRM	A Digital Rights Management (DRM) license allows media files only to be used on the devices authorized for those media files.
Dumpster Diving	The act of searching through a dumpster to look for proprietary or confidential information on a person or company.
Dynamic IP Address	An IP address that is leased to a device through a DHCP server.
Ease of Access	A Control Panel utility that provides accessibility features for people who need assistance in doing basic computer tasks.
EFS	Encrypting File System (EFS) encrypts files and folders on NTFS-formatted hard drives within Windows.
Endpoint Manager	A Microsoft-based tool that helps shape MDM policies for mobile devices on networks.
EOL	End-Of-Life (EOL) is a stage for a system or app to where the system or app is no longer supported by a vendor, meaning that it no longer receives updates, including security updates.
Equipment Grounding	The act of ensuring that equipment is not prone to static electricity while the equipment is being worked on.
ESD	Electrostatic Discharge (ESD) is the discharge of electrical currents from a device or a person and, left unmitigated, can reach and damage equipment.
ESD Mat	A mat that sits on top of a workbench or desk and on which a device sits to absorb static electricity so that the electricity does not reach computer components.
ESD Strap	A strap, worn around the wrist, which prevents a person from transferring static electricity to computer components.
EULA	An End-User License Agreement (EULA) dictates what people can and cannot do with a software license.
Event Viewer	A tool used to store system, application, and security logs on a Windows device.

Term	Definition
Evil Twin	A wireless access point set up, usually with the same SSID as a legitimate access point, with a goal of luring people into connecting to the twin and exploiting those people's devices.
exFAT	Extensible File Allocation Table (exFAT) is a file format that can be read on multiple operating systems, including Windows, Linux, and macOS.
Ext3	Third extended filesystem (ext3) is a Linux file system that supports a volume size up to 32 tebibytes and has a limit of 32,000 subdirectories.
Ext4	Fourth extended filesystem (ext4) is a Linux file system that supports very large volumes and has the ability to recover deleted files.
Extension	A two, three, or four-character mark on the end of a file which is used to identify a file's type and, in most cases, the app that works with the file.
Extension	An app or applet that add to a web browser's functionality.
Facial Recognition	A form of biometrics where one's face is used as an authentication mechanism to a device or system.
Failed Attempts Lockout	The locking out of a user account on a device or system after a failed number of sign in attempts to the device or system.
FAT32	File Allocation Table 32 (FAT32) is a file format that supports partitions up to 2 TB and a maximum file size of 32 GB.
FERPA	The Family Educational Rights and Privacy Act (FERPA) regulates how student records are handled within a school and school district.
File Server	A server dedicated to hosting files and folders and controlling permissions on those files and folders.
FileVault	A disk encryption service for macOS.
find	A Linux command that finds files within a folder.
Finder	A macOS feature that shows the location of apps, files, and folders on a macOS-based system.
Firmware	A set of instructions written into hardware on a device.
Folder Redirection	An Active Directory setting that allows for user account folders to change network locations instead of downloading to a device every time an account signs in to a different device.
Force Quit	A macOS feature that allows one to close an app when the app becomes unresponsive.
format	A command-line command used to erase data from a hard drive.
Full Backup	A backup that backs up all data slated for backup within a system or device.
Gaming	A settings area that allows one to set keyboard shortcuts for common gaming activities.
Gestures	A macOS feature that allows one to control how to navigate through macOS windows and apps based on hand gestures done on a touchpad.
GFS	Grandfather-Father-Son (GFS) is a backup scheme to where the son tapes are the daily tapes, the father tapes are weekly backups, and the grandfather tapes are monthly backups.
GLBA	The Gramm-Leach-Bliley Act (GLBA) defines privacy of customer information within financial institutions.
GPEdit	A console window that allows one to edit a Group Policy for a device, site, domain, or organizational unit.
gpresult	A command-line command used to show which Group Policies are applied to a device and the user account signed into the device.
GPU	A Graphics Processing Unit (GPU) is a processing chip on a video card and is used to avoid having a CPU process video instructions.
gpupdate	A command-line command used to update Group Policy on a device.
grep	A Linux command used to find specific or close to specific words or phrases of text within files.
Group Policy Editor	A tool used to create and modify Group Policies for a device or, in the case of a Windows Server, a device or group of devices within a domain.

Term	Definition
Guest User	A Windows user account that has limited access to a device in that the account cannot access system log files.
Hard Token	A small device with an LED that provides a code for an authentication factor to a system.
Hash	A one-way form of encryption where, once data is transmitted from a source to a destination, it can be encrypted again, and if the hashes match, the data has not been altered in any way.
Hibernate	A power state on a device where the device is in a low-power state with a snapshot of RAM taken and stored on a hard drive.
Hidden Files	Files that do not show in File Explorer unless the Show Hidden Files feature is enabled.
HIPAA	The Health Insurance Portability and Accountability Act (HIPAA) regulates how patient information is handled within the context of healthcare providers.
Home Folder	A default location for storing files and folders for a user account within Active Directory.
hostname	A command-line command that shows the name of a device.
Hot Swappable Drive	A hard drive that can be removed from a machine and replaced without having to turn the machine off.
Hyper-V Manager	Microsoft's version of a hypervisor. Hyper-V Manager can run multiple operating systems on multiple virtual machines.
Hypervisor	An app that uses physical resources on a device to host virtual machines on that device.
iCloud	The cloud storage app used in conjunction with Apple devices.
Image Deployment	An installation of Windows that copies a complete installation, including for apps and settings desired on machines in a business environment.
Impersonation	The act of someone pretending to be an authorized person in a communication situation.
Incident Report	A document that helps clarify and track incidents and their investigations.
Incremental Backup	A backup that backs up data changed since the most recent full or incremental backup.
Indexing Options	A Windows feature that allows for files to be cataloged, which makes files appear faster in search results.
Inheritance	In the context of permissions, a file or folder obtaining its ACL from a parent folder.
Insider Threat	A security threat involving someone inside a company, such as an employee or contractor.
Internet Options	An Internet Explorer window that allows one to control settings within Internet Explorer.
Invalid Certificate	A certificate that has either expired or been compromised, or both.
Inventory List	A list that tracks assets within a business.
iOS	An operating system, derived from macOS, found on iPhones.
IoT	The Internet of Things (IoT) is a means by which devices can be controlled remotely, usually through apps on mobile devices.
ip	A Linux command that, when run, returns IP address information on a device.
IP Address	The logical address of a device on a network.
iPadOS	An operating system, derived from macOS, found on iPads.
ipconfig	A command-line command that displays IP address information on a device.
ISO	An optical disc image (ISO) is an exact copy of a file that would ordinarily be found on a DVD or similar medium.
Jailbreak	The act of taking an iOS device and gaining access to perform premium features on the device.
Kerberos	An authentication mechanism that uses tokens to allow people who sign in to a domain to access multiple resources without having to sign on to each resource.
Key Fob	A small security token which is used to authenticate a person into a building or part of a building.
Keychain	A macOS feature that saves passwords for an Apple ID.
Keylogger	A tool used to capture keystrokes on a keyboard, with one purpose being to use that information to break into a system at a later date.

Term	Definition
Knowledge Base	A library of articles used to help solve device and app-related issues.
Linux	An open source operating system that comes in many editions and runs many apps and has many features.
Local Users and Groups	An area within Windows where local user accounts and groups can be created and managed and the group memberships can be managed.
Locator Application	An app, usually on a smartphone or tablet, that tracks the location of the smartphone or tablet.
Login Script	A script that maps user accounts to network resources upon a user account signing in to a domain.
Low-Level Formatting	A type of disk formatting that is done at a drive-making factory. This type of formatting sets up disk sectors on a magnetic hard drive to receive data.
ls	A Linux command that lists contents of a directory.
macOS	The operating system prevalent on Apple devices. macOS runs many apps and contains many features.
Magnetometer	A metal detector used to determine whether a person is carrying metal on their person.
Mail	In the context of applets, a Control Panel applet used to set up an Outlook mail profile for a user account on a device.
Malware	Malicious software that infects devices and corrupts and negatively affects files, folders, and overall systems.
man	A Linux command that, when run in conjunction with another command, shows information about that command, manual style.
Mapped Drive	A folder, usually on a remote device, that is assigned a drive letter on a local device.
md	A command-line command that creates a directory on a device.
MDM	Mobile Device Management (MDM) is a tool that sets policies for devices that will be allowed on a network, the requirements of those devices, and the apps that will be allowed on those devices.
Metered Connection	A network connection that limits the amount of data that can be transmitted over a specific time period.
MFA	Multifactor Authentication (MFA) is a form of authentication that requires two or more types of authentication information (what you know, what you have, who you are).
Microsoft Account	An account that can have its data and settings synchronized across devices and have its data stored in OneDrive.
Microsoft Store	An app from which Windows apps can be obtained. These apps are tested to make sure they are legitimate before being allowed in the store.
Microsoft Windows	A very popular workstation operating system that runs a very large variety of apps and features.
Mission Control	A macOS feature that allows one to have multiple desktops and control keyboard shortcuts to navigate through those desktops.
Motion Sensor	An infrared or similar device used to detect activity in an area of a building.
MSDS	A Material Safety Data Sheet (MSDS) is a document that defines how hazardous materials should be handled and disposed of and what should be done if these materials come in contact with someone.
MSRA	Microsoft Remote Assistance (MSRA) is an executable that allows a person to send invitations to someone else for a remote connection to a device.
mv	A Linux command that moves a file to another folder.
nano	A Linux-based text editor.
net use	A command-line command used to map a user account to a network drive.
net user	A command-line command used to get information on a user.
netstat	A command-line command that shows network statistics and open or listening ports on a device.

Term	Definition
Network and Internet	A settings area that allows for changing adapter options, controlling how devices are shared, and troubleshooting network problems.
Network and Sharing Center	A window that displays network adapters and their connections, with opportunity to see details of those connections.
Network Topology Diagram	A diagram that shows the physical placement of network devices and, in some cases, the logical makeup of a network.
Networks	On macOS, a window that allows one to configure wired and wireless network connections.
NFC	Near-Field Communication (NFC) is a connection service that allows devices within inches of each other to communicate with each other.
NFS	Network File System (NFS) is the primary protocol for sharing files and folders in Linux.
Non-Compliant System	A system that does not meet policy requirements to be allowed on a network.
Notifications Area	The area in the lower-right corner of a Windows desktop. The area displays messages for app and Windows updates and, if configured to do so, current events.
nslookup	An interactive command-line command that shows DNS information on a device or, if desired, a different device.
NTFS	New Technology File System (NTFS) is a file format common to Windows devices and supports granular, file-level security, compression, and encryption.
Offboarding	The process of recovering equipment and intellectual property from someone who leaves a company.
Onboarding	The process of acclimating a new hire to a business as quickly as possible so that the new hire can be productive immediately.
OneDrive	The cloud storage feature within Microsoft.
On-Path Attack	An attack in which a communication flow between two devices is intercepted and the data captured is either stolen or altered.
Open-Source License	A free license for software with code that can be altered and redistributed.
Organizational Unit	A logical grouping of users and devices within a domain, with the intent that policies can be set on this logical grouping.
Organizational Unit	A logical grouping of users, groups, devices, and policies within Active Directory.
Partition	A logical portion of a hard drive that is used to store data.
Partitioning	The logical splitting of a hard drive into separate areas for storing files, including, if warranted, installation files for an operating system.
Password Complexity	The definition of the number of characters and the number of character types required for a password.
Password Expiration	The amount of time a password can be used before it needs to be changed.
Password Manager	An app or tool that stores passwords people use to sign in to apps, websites, and systems.
pathping	A command-line command that shows hops on a route from source to destination and information on packets being sent or dropped at each hop.
PCI-DSS	The Payment Card Industry Data Security Standard (PCI-DSS) guides how businesses should handle data involving any debit or credit cards accepted for payment.
Performance Monitor	A tool used to show performance statistics on a devices, memory, network performance, physical disk performance, and processor performance.

Term	Definition
Perpetual License	A type of software license that never expires.
Personal Use License	A license for software that likely costs nothing but has restricted usage.
Personalization	A Windows setting that allows one to control a desktop background on a device.
PHI	Personal Health Information (PHI) is patient information that, if leaked, can be detrimental to patients and healthcare providers.
Phishing	A means by which attackers try to get personal or confidential information out of someone through email.
PII	Personally Identifiable Information (PII) is information tied to an individual. This information includes one's name, address, birthdate, and family information.
PIN	An alphanumeric code used as an authentication mechanism for a device or system.
ping	A command-line command that shows the ability of a host to connect to another host.
Plug-In	An app or applet that changes the way a webpage is loaded.
Pop-Up Blocker	A browser tool that prevents unwanted ads and browser windows from appearing on a device.
Port Forwarding	The act of directing traffic to a specific device on a network based on the incoming port number contained in the data packets being transmitted.
Power Options	A Control Panel applet which controls how power and performance related to power are managed on a device.
Power User	A Windows user account type that is provided for backward compatibility for Windows 7 and 8 but has the same permissions on a device as a standard account.
Pre-Shared Key	A password set to authenticate a device to a wireless network.
Principle of Least Privilege	A principle in which people are given permissions and rights necessary to do their jobs but no more than that.
Print Spooler	A service that controls print queues and processes print jobs on printers.
Privacy	In the context of settings, an area that allows one to control the appearance of advertisements and how much location tracking is used within apps on a device.
Private Browsing	The act of browsing webpages without having the browsing history saved on one's device.
Process Explorer	A tool that shows running processes and helps technicians identify rogue processes on a device.
Procurement Life Cycle	A sequence which covers an asset all throughout its lifespan, from identifying the need for the asset, to purchasing it, to supporting it until it is time to retire the asset.
Programs and Features	A Control Panel applet that allows one to modify, repair, and uninstall apps and enable or disable Windows features.
Proxy Server	A server that caches internet content and handles internet requests on behalf of client devices.
ps	A Linux command that shows processes a user account is running on a device.
pwd	A Linux command that displays the current working directory for a user account.
Quarantine	The act of isolating a system that is suspected of containing malware.
RADIUS	Remote Authentication Dial-in User Service (RADIUS) is a protocol used as a centralized source to control authentication, authorization, and accounting.
RAM	Random Access Memory (RAM) is a chip or multiple chips used for temporary storage inside a device.
Ransomware	A form of malware in which data is stolen and encrypted and then a demand is made for money for the data to be returned and decrypted.
RDP	Remote Desktop Protocol (RDP) is the Microsoft protocol used to host and connect to remote desktop sessions.
Recovery Mode	A Windows mode from which an operating system can be repaired or reinstalled.
Recovery Partition	A specific partition on a hard drive for storing files that aid in a Windows recovery, should one become necessary.

Term	Definition
Redirection	The automatic sending of a person from one website to another.
Registry Editor	A tool that stores every operating system and every app setting for every user account on a device. The editor allows for changing those settings.
Reimage	A task in which Windows is reinstalled on a device using a pre-built image containing the needed settings and apps for a person or department within a company.
Reliability Monitor	A Windows tool that shows warnings and failures for Windows applications.
Remediation	The process by which malware is removed from a device. This process can also describe steps taken to make a system compatible with network policies.
Remote Disc	A macOS feature that allows one to share out a CD or DVD drive and make it accessible to someone who presumably does not have a CD or DVD drive.
Remote Wipe	The act of restoring a device to its factory settings through remote means.
Request Form	In the context of change management, a form that contains a change request, its details, the risk analysis for the change, and a rollback plan in case the change does not work.
Resource Monitor	A tool that displays utilization of a device's CPU, RAM, disks, and network interfaces.
Risk Analysis	The establishing of a risk level and impact for a proposed change to a system, app, or both.
rm	A Linux command that deletes a file.
rmdir	A command-line command that removes a directory on a device.
RMM	Remote Monitoring and Management (RMM) is a tool that remotely monitors and manages infrastructures.
Roaming Profile	A group of settings, such as user account information, files, folders, and internet profiles, that follows a user account from device to device.
robocopy	A command-line command that allows for copying files and folders in many different ways.
Roll Back	The act of uninstalling an update to an app, hardware, or operating system.
Rollback Plan	A facet of change management that accounts for a change not working and a mechanism by which a system or process can be restored to its full functionality before a change took place.
Root Access	Superuser access to an Android device allowing one to install a different version of Android on a device.
Rootkit	A form of malware that accesses and corrupts administrative areas and system files on a device.
Run As	A Windows feature that allows a standard user to be elevated to an administrator mode for the purposes of running a specific app or an app with needed specific privileges.
SAE	Simultaneous Authentication of Equals (SAE) is an authentication mechanism for wireless networks and is faster than pre-shared keys, thus making SAE resistant to dictionary attacks.
Safe Mode	A state of Windows in which a minimal set of drivers is loaded. This state is often used when a thorough antimalware scan is run on a device.
Safety Goggles	A special pair of eyeglasses worn to protect eyes from dust and other flying particles while working on equipment.
Samba	A Linux tool, used as a directory service, that supports SMB.
Sandbox Testing	The act of testing a change to an app, process, or system in an environment isolated from the production environment of a business.
Screened Subnet	Also known as a demilitarized zone (DMZ), a logical portion of a network that contains devices that need to communicate both with an internal or private portion of a network and an external or public portion of a network.
Screensaver Lock	A screensaver that appears on a screen after a determined length of time, requiring a password to shut off the screensaver.

Term	Definition
Security Group	A group, containing users, that can be assigned permissions and be assigned to organizational units, with the purpose being that groups are easier to manage than are individual user accounts.
Service	A process that helps apps and other processes run on a device.
setx	A Windows command that can make changes to a system registry.
sfc	System File Checker (SFC) is a command-line command that is used to check and, if needed, repair or replace system files.
Shared Resource	A resource, such as a folder, that is accessible to multiple people and groups.
Shoulder Surfing	A spy tactic, used by an attacker, in which the attacker peers over one's shoulder to steal information from that person.
Shredding	The act of making paper documents unrecognizable through converting them into very small bits of paper.
shutdown	A command-line command that shuts down and, if warranted, restarts a device.
Sleep Mode	A device mode to where a device is seemingly off but is actually in a low-power state.
Smart Card	A credit card-like device with a chip, which stores authentication information, thus allowing someone access to a building according to the permissions stored on the chip.
SMB	Server Message Block (SMB) is the primary protocol for sharing files and folders in Windows.
SMS	Short Message Service (SMS) is the protocol for text messaging on mobile devices.
Soft Token	An app that provides a code for an authentication factor to a system.
SOP	A Standard Operating Procedure (SOP) document outlines a how-to for a business process.
Sound	In the context of applets, a Control Panel applet that allows one to choose and configure audio devices on a computer.
SOX	The Sarbanes-Oxley Act (SOX) regulates how publicly traded companies maintain and protect financial data.
Splash Screen	A screen that appears when one starts up a device.
Spoofing	An attempt by a person or group to masquerade as someone else, or an attack using a device that is attempting to masquerade itself as something else.
Spotlight	A macOS feature that allows one to search for a topic and get results from many sources.
Spyware	A form of malware in which a tool gathers information on one's apps used, webpages visited, and similar information for what a person does on a device.
SQL Injection	The addition of Structured Query Language (SQL) code to a form field or the end of a URL with the code being an attempt to retrieve data from or change data in a database.
SQL Server	A Microsoft database app that hosts and stores relational databases.
SSH	Secure Shell (SSH) is a protocol that offers a secure connection between two devices.
SSID	A Service Set Identifier (SSID) is an identity for a wireless network.
SSID Broadcast	The advertising of an SSID to devices looking to connect to a wireless network.
SSO	Single Sign-On (SSO) allows a person to have a single form of authentication be used across multiple apps, systems, or devices.
Standard Account	A Windows account that can create and manage files and folders and can install apps on devices.
Standby Mode	A device mode where a display turns off after a period of inactivity.
Static IP Address	An IP address that is assigned manually to a device, with the intention that the IP address will not change.
Static WAN	A public IP address assigned statically to a router that connects to the internet.
su	A Linux command that switches a user account on a device.
Subnet Mask	The portion of an IP address that defines the network portion of the address and the node portion of the address. A subnet mask also determines the number of devices that are allowed on a network.

Term	Definition
sudo	A Linux command that gives a person a superuser designation to run commands that require a superuser designation.
Surge Suppressor	A specialized power strip used to regulate power sent to devices.
Synthetic Backup	A type of full backup in which changes are made to a previous full backup rather than a new full backup being created.
System	A Control Panel utility that allows for copying machine specs, for initiating an upgrade, and for settings that can be utilized to adjust and improve device performance.
System Configuration	A Windows tool that allows one to control how a device starts up.
System Information	A window that displays system specifications, including name, manufacturer, processor, BIOS/UEFI information, RAM, drives, and network devices.
System Preferences	An area within macOS that contains many system-based apps and tools used to keep a macOS device up to date.
System Restore	A mechanism by which a system's registry can be restored to a point in time, hopefully before a malicious app or malware was installed on a device.
TACACS+	Terminal Access Controller Access Control System (TACACS)+ is a protocol, developed by Cisco, which is used for authentication to routers and managed switches.
Tailgating	The act of an unauthorized person entering a secure location right behind an authorized person who has used credentials to enter that location.
Task Manager	An app that shows the CPU, memory, disk, and network usage on a device. The app also shows running processes on a device.
Task Scheduler	A tool used to schedule processes that are determined to need to run on a regular basis or as a result of a specific event on a device.
Terminal	In Linux and Mac, the app in which commands are run in a command-line environment.
Ticketing System	An app or form that stores problems, details, and solutions for hardware and software problems within an infrastructure.
Time and Language	A Control Panel applet used to set the time, time zone, default language, and languages used on a device.
Time Drift	An occurrence of a system clock on a system board becoming inaccurate, which affects how a device interacts with other devices on a network.
Time Machine	A macOS mechanism that backs up an entire hard drive and allows one to set up a schedule for backing up a hard drive.
top	A Linux command that shows a list of processes a user account is running on a device and gives one an opportunity to terminate a process.
tracert	A command-line command used to show hops from a source to destination and, if necessary, show where data transmissions are stopping on the way to a destination.
Trojan	An imposter program masquerading as a legitimate program.
UAC	User Account Control (UAC) is a tool used to elevate an account with standard privileges to administrator privileges temporarily when necessary.
UEFI	The Unified Extensible Firmware Interface (UEFI) is a graphical user interface version of a BIOS.
Update and Security	A Windows settings feature that installs security fixes and overall updates to Windows. This feature also encompasses virus and threat protection on a device.
Upgrade Path	A means in which one can get to either a newer version of Windows or a different edition of Windows within its own version, such as moving from Windows 10 Home to Windows 10 Pro.
UPnP	Universal Plug and Play (UPnP) allows devices to open ports for apps dynamically and allows for automatic port forwarding. UPnP is usually found on wireless access points.

Term	Definition
UPS	An Uninterruptible Power Supply (UPS) is a short term, battery-based power source that is used to keep systems up for a short time after a power outage.
USB Controller	A peripheral that hosts USB connections and controls the workload of USB devices connected to a system.
USB Lock	A lock which plugs into a USB port and prevents devices from connecting to the port, minimizing risk of data loss through the USB port.
USB Selective Suspend	A USB setting where a USB hub inside a device can suspend power to external devices when power is not needed on those devices.
User Account	An account that, on a device, has its own username, password, settings, folders, and files.
User Preferences	Settings on a device that help a user perform needed tasks optimally on a device.
Video Surveillance	The use of cameras and closed circuit television (CCTV) to monitor activity in a secure area of a building.
Virtual Memory	A portion of a hard disk that is used as RAM when the physical RAM on a device reaches its maximum capacity.
Virus	A form of malware that requires a carrier to propagate through a system or multiple systems.
Vishing	A means by which attackers use Voice over IP (VoIP) to get personal or confidential information from someone.
VM Workstation Player	A virtual machine hypervisor that can run multiple operating systems on multiple virtual machines.
VNC	Virtual Network Computer (VNC) is a remote connection protocol that allows two devices to connect to each other and, during the connection, one can observe what the other person is doing.
VoIP	Voice over IP (VoIP) is a system of voice communication using digital signals.
Volume Licensing	A licensing structure where a licensing purchase can cover all users within a business.
VPN	A Virtual Private Network (VPN) is a secure network tunnel within a public network.
Warranty	The coverage of an asset should an asset stop functioning properly or break.
Whaling	A form of phishing that targets someone of importance, like a company CEO.
Windows 10 Enterprise	An edition of Windows that has features to protect machines in a business environment and supports volume licensing.
Windows 10 Home	An edition of Windows that is built for average home systems and does not support business-oriented features.
Windows 10 Pro	An edition of Windows that supports business features such as BitLocker, hosting Remote sessions, and joining a domain.
Windows 10 Pro for Workstations	An edition of Windows that has all the features of Windows Pro and supports up to 6 TB of RAM.
Windows Compatible Products List	A searchable database online that displays, for Windows editions, the compatibility of hardware devices with the Windows editions.
Windows Defender	An antimalware app that comes pre-installed with Windows and is the default antimalware app unless another antimalware app is installed.
Windows Defender Firewall	An app that helps to control incoming and outgoing traffic on a device, with criteria consisting mainly of ports and protocols.
Windows Profile	A group of settings, such as user account information, files, folders, and internet profiles, that resides on a device hosting a user account.
Windows Security	A centrally-themed tool used as a gateway to security tools such as a firewall and antimalware apps.
Winver	A command-line command that displays the version of Windows running on a device.

Term	Definition
Workgroup	A type of network in which each device has its own set of user accounts and permissions for resources.
WPA2	WiFi Protected Access 2 (WPA2) is a wireless security protocol that uses 128-bit AES to protect data on a wireless network.
WPA3	WiFi Protected Access 3 (WPA3) is a wireless security protocol that uses the Simultaneous Authentication of Equals (SAE) exchange for authentication.
WWAN	A Wireless Wide Area Network (WWAN) is a network where a device is connected to the network directly through a cellular connection.
xcopy	A command-line command that copies files and folders from one location to another.
Xprotect	A built-in antivirus package for systems using macOS.
yum	A Linux command, used on some versions of Linux, that runs installation packages on devices.
Zero-Day Attack	An attack in which an exploit is done on one or more devices or apps with the device or app builder having no knowledge of the security vulnerability being attacked.
Zombie	A computer that has been taken over by an attacker and is used, along with other computers, to carry out DDoS attacks.

Objectives

Domain 1 Operating Systems	Domain 2 Security	Domain 3 Software Troubleshooting	Domain 4 Operational Procedures
1.1 Identify basic features of Microsoft Windows editions 1.1.1 Windows 10 editions 1.1.1.1 Home 1.1.1.2 Pro 1.1.1.3 Pro for Workstations 1.1.1.4 Enterprise 1.1.2 Feature differences 1.1.2.1 Domain access vs. workgroup 1.1.2.2 Desktop styles/user interface 1.1.2.3 Availability of Remote Desktop Protocol (RDP) 1.1.2.4 Random-access memory (RAM) support limitations 1.1.2.5 BitLocker 1.1.2.6 Gpedit.msc 1.1.3 Upgrade paths 1.1.3.1 In-place upgrade	2.1 Summarize various security measures and their purposes 2.1.1 Physical security 2.1.1.1 Access control vestibule 2.1.1.2 Badge reader 2.1.1.3 Video surveillance 2.1.1.4 Alarm systems 2.1.1.5 Motion sensors 2.1.1.6 Door locks 2.1.1.7 Equipment locks 2.1.1.8 Guards 2.1.1.9 Bollards 2.1.1.10 Fences 2.1.2 Physical security for staff 2.1.2.1 Key fobs 2.1.2.2 Smart cards 2.1.2.3 Keys 2.1.2.4 Biometrics 2.1.2.4.1 Retina scanner 2.1.2.4.2 Fingerprint scanner 2.1.2.4.3 Palmprint scanner 2.1.2.5 Lighting 2.1.2.6 Magnetometers 2.1.3 Logical security 2.1.3.1 Principle of least privilege 2.1.3.2 Access control lists (ACLs) 2.1.3.3 Multifactor authentication (MFA) 2.1.3.4 Email 2.1.3.5 Hard token 2.1.3.6 Soft token 2.1.3.7 Short message service (SMS) 2.1.3.8 Voice call 2.1.3.9 Authenticator application 2.1.4 Mobile device management (MDM) 2.1.5 Active Directory 2.1.5.1 Log0n script 2.1.5.2 Domain 2.1.5.3 Group Policy/updates 2.1.5.4 Organizational units 2.1.5.5 Home folder 2.1.5.6 Folder redirection 2.1.5.7 Security groups	3.1 Given a scenario, troubleshoot common Windows OS problems 3.1.1 Common symptoms 3.1.1.1 Blue screen of death (BSOD) 3.1.1.2 Sluggish performance 3.1.1.3 Boot problems 3.1.1.4 Frequent shutdowns 3.1.1.5 Services not starting 3.1.1.6 Applications crashing 3.1.1.7 Low memory warnings 3.1.1.8 USB controller resource warnings 3.1.1.9 System instability 3.1.1.10 No OS found 3.1.1.11 Slow profile load 3.1.1.12 Time drift 3.1.2 Common troubleshooting steps 3.1.2.1 Reboot 3.1.2.2 Restart services 3.1.2.3 Uninstall/reinstall/update applications 3.1.2.4 Add resources 3.1.2.5 Verify requirements 3.1.2.6 System file check 3.1.2.7 Repair Windows 3.1.2.8 Restore 3.1.2.9 Reimage 3.1.2.10 Roll back updates 3.1.2.11 Rebuild Windows profiles	4.1 Given a scenario, implement best practices associated with documentation and support systems information management 4.1.1 Ticketing systems 4.1.1.1 User information 4.1.1.2 Device information 4.1.1.3 Description of problems 4.1.1.4 Categories 4.1.1.5 Severity 4.1.1.6 Escalation levels 4.1.1.7 Clear, concise written communication 4.1.1.7.1 Problem description 4.1.1.7.2 Progress notes 4.1.1.7.3 Problem resolution 4.1.2 Asset management 4.1.2.1 Inventory lists 4.1.2.2 Database system 4.1.2.3 Asset tags and IDs 4.1.2.4 Procurement life cycle 4.1.2.5 Warranty and licensing 4.1.2.6 Assigned users 4.1.3 Types of documents 4.1.3.1 Acceptable use policy (AUP) 4.1.3.2 Network topology diagram 4.1.3.3 Regulatory compliance requirements 4.1.3.3.1 Splash screens 4.1.3.4 Incident reports 4.1.3.5 Standard operating procedures 4.1.3.5.1 Procedures for custom installation of software package 4.1.3.6 New user setup checklist 4.1.3.7 End user termination checklist 4.1.4 Knowledge base/articles

Domain 1 Operating Systems	Domain 2 Security	Domain 3 Software Troubleshooting	Domain 4 Operational Procedures
1.2 Given a scenario, use the appropriate Microsoft command-line tool 1.2.1 Navigation 1.2.1.1 cd 1.2.1.2 dir 1.2.1.3 md 1.2.1.4 rmdir 1.2.1.5 Drive navigation inputs: 1.2.1.5.1 C: or D: or X: 1.2.2 Command-line tools 1.2.2.1 ipconfig 1.2.2.2 ping 1.2.2.3 hostname 1.2.2.4 netstat 1.2.2.5 nslookup 1.2.2.6 chkdsk 1.2.2.7 net user 1.2.2.8 net use 1.2.2.9 tracert 1.2.2.10 format 1.2.2.11 xcopy 1.2.2.12 copy 1.2.2.13 robocopy 1.2.2.14 gpupdate 1.2.2.15 gpresult 1.2.2.16 shutdown 1.2.2.17 Sfc 1.2.2.18 [command name] /? 1.2.2.19 diskpart 1.2.2.20 pathping 1.2.2.21 Winver	2.2 Compare and contrast wireless security protocols and authentication methods 2.2.1 Protocols and encryption 2.2.1.1 WiFi Protected Access 2 (WPA2) 2.2.1.2 WPA3 2.2.1.3 Temporal Key Integrity Protocol (TKIP) 2.2.1.4 Advanced Encryption Standard (AES) 2.2.2 Authentication 2.2.2.1 Remote Authentication Dial-In User Service (RADIUS) 2.2.2.2 Terminal Access Controller Access-Control System (TACACS+) 2.2.2.3 Kerberos 2.2.2.4 Multifactor	3.2 Given a scenario, troubleshoot common personal computer (PC) security issues 3.2.1 Common symptoms 3.2.1.1 Unable to access the network 3.2.1.2 Desktop alerts 3.2.1.3 False alerts regarding antivirus protection 3.2.1.4 Altered system or personal files 3.2.1.4.1 Missing/renamed files 3.2.1.5 Unwanted notifications within the OS 3.2.1.6 OS update failures 3.2.2 Browser-related symptoms 3.2.2.1 Random/frequent pop-ups 3.2.2.2 Certificate warnings 3.2.2.3 Redirection	4.2 Explain basic change-management best practices 4.2.1 Documented business processes 4.2.1.1 Rollback plan 4.2.1.2 Sandbox testing 4.2.1.3 Responsible staff member 4.2.2 Change management 4.2.2.1 Request forms 4.2.2.2 Purpose of the change 4.2.2.3 Scope of the change 4.2.2.4 Date and time of the change 4.2.2.5 Affected systems/impact 4.2.2.6 Risk analysis 4.2.2.6.1 Risk level 4.2.2.7 Change board approvals 4.2.2.8 End-user acceptance

Domain 1 Operating Systems	Domain 2 Security	Domain 3 Software Troubleshooting	Domain 4 Operational Procedures
1.3 Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS) 1.3.1 Task Manager 1.3.1.1 Services 1.3.1.2 Startup 1.3.1.3 Performance 1.3.1.4 Processes 1.3.1.5 Users 1.3.2 Microsoft Management Console (MMC) snap-in 1.3.2.1 Event Viewer (eventvwr.msc) 1.3.2.2 Disk Management (diskmgmt.msc) 1.3.2.3 Task Scheduler (taskschd.msc) 1.3.2.4 Device Manager (devmgmt.msc) 1.3.2.5 Certificate Manager (certmgr.msc) 1.3.2.6 Local Users and Groups (lusrmgr.msc) 1.3.2.7 Performance Monitor (perfmon.msc) 1.3.2.8 Group Policy Editor (gpedit.msc) 1.3.3 Additional tools 1.3.3.1 System Information (msinfo32.exe) 1.3.3.2 Resource Monitor (resmon.exe) 1.3.3.3 System Configuration (msconfig.exe) 1.3.3.4 Disk Cleanup (cleanmgr.exe) 1.3.3.5 Disk Defragment (dfrgui.exe) 1.3.3.6 Registry Editor (regedit.exe)	2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods 2.3.1 Malware 2.3.1.1 Trojan 2.3.1.2 Rootkit 2.3.1.3 Virus 2.3.1.4 Spyware 2.3.1.5 Ransomware 2.3.1.6 Keylogger 2.3.1.7 Boot sector virus 2.3.1.8 Cryptominers 2.3.2 Tools and methods 2.3.2.1 Recovery mode 2.3.2.2 Antivirus 2.3.2.3 Antimalware 2.3.2.4 Software firewalls 2.3.2.5 Anti-phishing training 2.3.2.6 User education regarding common threats 2.3.2.7 OS reinstallation	3.3 Given a scenario, use best practice procedures for malware removal 3.3.1 1. Investigate and verify malware symptoms 3.3.2 2. Quarantine infected systems 3.3.3 3. Disable System Restore in Windows 3.3.4 Remediate infected systems 3.3.4.1 Update antimalware software 3.3.4.2 Scanning and removal techniques (e.g., safe mode, preinstallation environment) 3.3.5 Schedule scans and run updates 3.3.6 Enable System Restore and create a restore point in Windows 3.3.7 Educate the end user	4.3 Given a scenario, implement workstation backup and recovery methods 4.3.1 Backup and recovery 4.3.1.1 Full 4.3.1.2 Incremental 4.3.1.3 Differential 4.3.1.4 Synthetic 4.3.2 Backup testing 4.3.2.1 Frequency 4.3.3 Backup rotation schemes 4.3.3.1 On-site vs. off-site 4.3.3.2 Grandfather-Father-Son (GFS) 4.3.3.3 3-2-1 backup rule

Domain 1 Operating Systems	Domain 2 Security	Domain 3 Software Troubleshooting	Domain 4 Operational Procedures
1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility 1.4.1 Internet Options 1.4.2 Devices and Printers 1.4.3 Programs and Features 1.4.4 Network and Sharing Center 1.4.5 System 1.4.6 Windows Defender Firewall 1.4.7 Mail 1.4.8 Sound 1.4.9 User Accounts 1.4.10 Device Manager 1.4.11 Indexing Options 1.4.12 Administrative Tools 1.4.13 File Explorer options 1.4.13.1 Show hidden files 1.4.13.2 Hide extensions 1.4.13.3 General options 1.4.13.4 View options 1.4.14 Power options 1.4.14.1 Hibernate 1.4.14.2 Power plans 1.4.14.3 Sleep/suspend 1.4.14.4 Standby 1.4.14.5 Choose what closing the lid does 1.4.14.6 Turn on fast startup 1.4.14.7 Universal Serial Bus (USB) selective suspend 1.4.15 Ease of Access	2.4 Explain common social-engineering attacks, threats, and vulnerabilities 2.4.1 Social engineering 2.4.1.1 Phishing 2.4.1.2 Vishing 2.4.1.3 Shoulder surfing 2.4.1.4 Whaling 2.4.1.5 Tailgating 2.4.1.6 Impersonation 2.4.1.7 Dumpster diving 2.4.1.8 Evil twin 2.4.2 Threats 2.4.2.1 Distributed denial of service (DDoS) 2.4.2.2 Denial of Service (DoS) 2.4.2.3 Zero-day attack 2.4.2.4 Spoofing 2.4.2.5 On-path attack 2.4.2.6 Brute-force attack 2.4.2.7 Dictionary attack 2.4.2.8 Insider threat 2.4.2.9 Structured Query Language (SQL) injection 2.4.3 Vulnerabilities 2.4.3.1 Non-compliant systems 2.4.3.2 Unpatched systems 2.4.3.3 Unprotected systems (missing antivirus/missing firewall) 2.4.3.4 EOL OSs 2.4.3.5 Bring your own device (BYOD)	3.4 Given a scenario, troubleshoot common mobile OS and application issues 3.4.1 Common symptoms 3.4.1.1 Application fails to launch 3.4.1.2 Application fails to close/crashes 3.4.1.3 Application fails to update 3.4.1.4 Slow to respond 3.4.1.5 OS fails to update 3.4.1.6 Battery life issues 3.4.1.7 Randomly reboots 3.4.1.8 Connectivity issues 3.4.1.8.1 Bluetooth 3.4.1.8.2 Wi-Fi 3.4.1.8.3 Near-field communication (NFC) 3.4.1.8.4 AirDrop 3.4.1.9 Screen does not autorotate	4.4 Given a scenario, use common safety procedures 4.4.1 Electrostatic discharge (ESD) straps 4.4.2 ESD mats 4.4.3 Equipment grounding 4.4.4 Proper power handling 4.4.5 Proper component handling and storage 4.4.6 Antistatic bags 4.4.7 Compliance with government regulations 4.4.8 Personal safety 4.4.8.1 Disconnect power before repairing PC 4.4.8.2 Lifting techniques 4.4.8.3 Electrical fire safety 4.4.8.4 Safety goggles 4.4.8.5 Air filtration mask

Domain 1 **Operating Systems**	**Domain 2** **Security**	**Domain 3** **Software Troubleshooting**	**Domain 4** **Operational Procedures**
1.5 Given a scenario, use the appropriate Windows settings 1.5.1 Time & Language 1.5.2 Update & Security 1.5.3 Personalization 1.5.4 Apps 1.5.5 Privacy 1.5.6 System 1.5.7 Devices 1.5.8 Network & Internet 1.5.9 Gaming 1.5.10 Accounts	2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS 2.5.1 Defender Antivirus 2.5.1.1 Activate/deactivate 2.5.1.2 Updated definitions 2.5.2 Firewall 2.5.2.1 Activate/deactivate 2.5.2.2 Port security 2.5.2.3 Application security 2.5.3 Users and groups 2.5.3.1 Local vs. Microsoft account 2.5.3.2 Standard account 2.5.3.3 Administrator 2.5.3.4 Guest user 2.5.3.3 Power user 2.5.4 Login OS options 2.5.4.1 Username and password 2.5.4.2 Personal identification number (PIN) 2.5.4.3 Fingerprint 2.5.4.4 Facial recognition 2.5.4.5 Single sign-on (SSO) 2.5.5 NTFS vs. share permissions 2.5.5.1 File and folder attributes 2.5.5.2 Inheritance 2.5.6 Run as administrator vs. standard user 2.5.6.1 User Account Control (UAC) 2.5.7 BitLocker 2.5.8 BitLocker To Go 2.5.9 Encrypting File System (EFS)	3.5 Given a scenario, troubleshoot common mobile OS and application security issues 3.5.1 Security concerns 3.5.1.1 Android package (APK) source 3.5.1.2 Developer mode 3.5.1.3 Root access/jailbreak 3.5.1.4 Bootleg/malicious application 3.5.1.4.1 Application spoofing 3.5.2 Common symptoms 3.5.2.1 High network traffic 3.5.2.2 Sluggish response time 3.5.2.3 Data-usage limit notification 3.5.2.4 Limited internet connectivity 3.5.2.5 No internet connectivity 3.5.2.6 High number of ads 3.5.2.7 Fake security warnings 3.5.2.8 Unexpected application behavior 3.5.2.9 Leaked personal files/data	4.5 Summarize environmental impacts and local environmental controls 4.5.1 Material safety data sheet (MSDS)/documentation for handling and disposal 4.5.1.1 Proper battery disposal 4.5.1.2 Proper toner disposal 4.5.1.3 Proper disposal of other devices and assets 4.5.2 Temperature, humidity-level awareness, and proper ventilation 4.5.2.1 Location/equipment placement 4.5.2.2 Dust cleanup 4.5.2.3 Compressed air/vacuums 4.5.3 Power surges, under-voltage events, and power failures 4.5.3.1 Battery backup 4.5.3.2 Surge suppressor

Domain 1 Operating Systems	Domain 2 Security	Domain 3 Software Troubleshooting	Domain 4 Operational Procedures
1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop 1.6.1 Workgroup vs. domain setup 1.6.1.1 Shared resources 1.6.1.2 Printers 1.6.1.3 File servers 1.6.1.4 Mapped drives 1.6.2 Local OS firewall settings 1.6.2.1 Application restrictions and exceptions 1.6.2.2 Configuration 1.6.3 Client network configuration 1.6.3.1 Internet Protocol (IP) addressing scheme 1.6.3.2 Domain Name System (DNS) 1.6.3.3 Subnet mask 1.6.3.4 Gateway 1.6.3.5 Static vs. dynamic 1.6.4 Establish network connections 1.6.4.1 Virtual private network (VPN) 1.6.4.2 Wireless 1.6.4.3 Wired 1.6.4.4 Wireless wide area network (WWAN) 1.6.5 Proxy settings 1.6.6 Public network vs. private network 1.6.7 File Explorer navigation – network paths 1.6.8 Metered connections and limitations	2.6 Given a scenario, configure a workstation to meet best practices for security 2.6.1 Data-at-rest encryption 2.6.2 Password best practices 2.6.2.1 Complexity requirements 2.6.2.1.1 Length 2.6.2.1.2 Character types 2.6.2.2 Expiration requirements 2.6.2.3 Basic input/output system (BIOS)/ Unified Extensible Firmware Interface (UEFI) passwords 2.6.3 End-user best practices 2.6.3.1 Use screensaver locks 2.6.3.2 Log off when not in use 2.6.3.3 Secure/protect critical hardware (e.g., laptops) 2.6.3.4 Secure personally identifiable information (PII) and passwords 2.6.4 Account management 2.6.4.1 Restrict user permissions 2.6.4.2 Restrict login times 2.6.4.3 Disable guest account 2.6.4.4 Use failed attempts lockout 2.6.4.5 Use timeout/screen lock 2.6.5 Change default administrator's user account/password 2.6.6 Disable AutoRun 2.6.7 Disable AutoPlay		4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts 4.6.1 Incident response 4.6.1.1 Chain of custody 4.6.1.2 Inform management/law enforcement as necessary 4.6.1.3 Copy of drive (data integrity and preservation) 4.6.1.4 Documentation of incident 4.6.2 Licensing/digital rights management (DRM)/end-user license agreement (EULA) 4.6.2.1 Valid licenses 4.6.2.2 Non-expired licenses 4.6.2.3 Personal use license vs. corporate use license 4.6.2.4 Open-source license 4.6.3 Regulated data 4.6.3.1 Credit card transactions 4.6.3.2 Personal government-issued information 4.6.3.3 PII 4.6.3.4 Healthcare data 4.6.3.5 Data retention requirements

Domain 1 Operating Systems	Domain 2 Security	Domain 3 Software Troubleshooting	Domain 4 Operational Procedures
1.7 Given a scenario, apply application installation and configuration concepts 1.7.1 System requirements for applications 1.7.1.1 32-bit vs. 64-bit dependent application requirements 1.7.1.2 Dedicated graphics card vs. integrated 1.7.1.3 Video random-access memory (VRAM) requirements 1.7.1.4 RAM requirements 1.7.1.5 Central processing unit (CPU) requirements 1.7.1.6 External hardware tokens 1.7.1.7 Storage requirements 1.7.2 OS requirements for applications 1.7.2.1 Application to OS compatibility 1.7.2.2 32-bit vs. 64-bit OS 1.7.3 Distribution methods 1.7.3.1 Physical media vs. downloadable 1.7.3.2 ISO mountable 1.7.4 Other considerations for new applications 1.7.4.1 Impact to device 1.7.4.2 Impact to network 1.7.4.3 Impact to operation 1.7.4.4 Impact to business	2.7 Explain common methods for securing mobile and embedded devices 2.7.1 Screen locks 2.7.1.1 Facial recognition 2.7.1.2 PIN codes 2.7.1.3 Fingerprint 2.7.1.4 Pattern 2.7.1.5 Swipe 2.7.2 Remote wipes 2.7.3 Locator applications 2.7.4 OS updates 2.7.5 Device encryption 2.7.6 Remote backup applications 2.7.7 Failed login attempts restrictions 2.7.8 Antivirus/anti-malware 2.7.9 Firewalls 2.7.10 Policies and procedures 2.7.10.1 BYOD vs. corporate owned 2.7.10.2 Profile security requirements 2.7.11 Internet of Things (IoT)		4.7 Given a scenario, use proper communication techniques and professionalism 4.7.1 Professional appearance and attire 4.7.1.1 Match the required attire of the given environment 4.7.1.1.1 Formal 4.7.1.1.2 Business casual 4.7.2 Use proper language and avoid jargon, acronyms, and slang, when applicable 4.7.3 Maintain a positive attitude/project confidence 4.7.4 Actively listen, take notes, and avoid interrupting the customer 4.7.5 Be culturally sensitive 4.7.5.1 Use appropriate professional titles, when applicable 4.7.6 Be on time (if late, contact the customer) 4.7.7 Avoid distractions 4.7.7.1 Personal calls 4.7.7.2 Texting/social media sites 4.7.7.3 Personal interruptions 4.7.8 Dealing with difficult customers or situations 4.7.8.1 Do not argue with customers or be defensive 4.7.8.2 Avoid dismissing customer problems 4.7.8.3 Avoid being judgmental 4.7.8.4 Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding) 4.7.8.5 Do not disclose experience via social media outlets 4.7.9 Set and meet expectations/timeline and communicate status with the customer 4.7.9.1 Offer repair/replacement options, as needed 4.7.9.2 Provide proper documentation on the services provided 4.7.9.3 Follow up with customer/user at a later date to verify satisfaction 4.7.10 Deal appropriately with customers' confidential and private materials 4.7.10.1 Located on a computer, desktop, printer, etc.

Domain 1 Operating Systems	Domain 2 Security	Domain 3 Software Troubleshooting	Domain 4 Operational Procedures
1.8 Explain common OS types and their purposes 1.8.1 Workstation OSs 1.8.1.1 Windows 1.8.1.2 Linux 1.8.1.3 macOS 1.8.1.4 Chrome OS 1.8.2 Cell phone/tablet OSs 1.8.2.1 iPadOS 1.8.2.2 iOS 1.8.2.3 Android 1.8.3 Various filesystem types 1.8.3.1 New Technology File System (NTFS) 1.8.3.2 File Allocation Table 32 (FAT32) 1.8.3.3 Third extended filesystem (ext3) 1.8.3.4 Fourth extended filesystem (ext4) 1.8.3.5 Apple File System (APFS) 1.8.3.6 Extensible File Allocation Table (exFAT) 1.8.4 Vendor life-cycle limitations 1.8.4.1 End-of-life (EOL) 1.8.4.2 Update limitations 1.8.5 Compatibility concerns between OSs	2.8 Given a scenario, use common data destruction and disposal methods 2.8.1 Physical destruction 2.8.1.1 Drilling 2.8.1.2 Shredding 2.8.1.3 Degaussing 2.8.1.4 Incinerating 2.8.2 Recycling or repurposing best practices 2.8.2.1 Erasing/wiping 2.8.2.2 Low-level formatting 2.8.2.3 Standard formatting 2.8.3 Outsourcing concepts 2.8.3.1 Third-party vendor 2.8.3.2 Certification of destruction/recycling		4.8 Identify the basics of scripting 4.8.1 Script file types 4.8.1.1 .bat 4.8.1.2 .ps1 4.8.1.3 .vbs 4.8.1.4 .sh 4.8.1.5 .js 4.8.1.6 .py 4.8.2 Use cases for scripting 4.8.2.1 Basic automation 4.8.2.2 Restarting machines 4.8.2.3 Remapping network drives 4.8.2.4 Installation of applications 4.8.2.5 Automated backups 4.8.2.6 Gathering of information/data 4.8.2.7 Initiating updates 4.8.3 Other considerations when using scripts 4.8.3.1 Unintentionally introducing malware 4.8.3.2 Inadvertently changing system settings 4.8.3.3 Browser or system crashes due to mishandling of resources

Domain 1 Operating Systems	Domain 2 Security	Domain 3 Software Troubleshooting	Domain 4 Operational Procedures
1.9 Given a scenario, perform OS installations and upgrades in a diverse OS environment 1.9.1 Boot methods 1.9.1.1 USB 1.9.1.2 Optical media 1.9.1.3 Network 1.9.1.4 Solid-state/flash drives 1.9.1.5 Internet-based 1.9.1.6 External/hot-swappable drive 1.9.1.7 Internal hard drive (partition) 1.9.2 Types of installations 1.9.2.1 Upgrade 1.9.2.2 Recovery partition 1.9.2.3 Clean install 1.9.2.4 Image deployment 1.9.2.5 Repair installation 1.9.2.6 Remote network installation 1.9.2.7 Other considerations 1.9.2.7.1 Third-party drivers 1.9.3 Partitioning 1.9.3.1 GUID [globally unique identifier] Partition Table (GPT) 1.9.3.2 Master boot record (MBR) 1.9.4 Drive format 1.9.5 Upgrade considerations 1.9.5.1 Backup files and user preferences 1.9.5.2 Application and driver support/backward compatibility 1.9.5.3 Hardware compatibility 1.9.6 Feature updates 1.9.6.1 Product life cycle	2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks 2.9.1 Home router settings 2.9.1.1 Change default passwords 2.9.1.2 IP filtering 2.9.1.3 Firmware updates 2.9.1.4 Content filtering 2.9.1.5 Physical placement/secure locations 2.9.1.6 Dynamic Host Configuration Protocol (DHCP) reservations 2.9.1.7 Static wide-area network (WAN) IP 2.9.1.8 Universal Plug and Play (UPnP) 2.9.1.9 Screened subnet 2.9.2 Wireless specific 2.9.2.1 Changing the service set identifier (SSID) 2.9.2.2 Disabling SSID broadcast 2.9.2.3 Encryption settings 2.9.2.4 Disabling guest access 2.9.2.5 Changing channels 2.9.3 Firewall settings 2.9.3.1 Disabling unused ports 2.9.3.2 Port forwarding/mapping		4.9 Given a scenario, use remote access technologies 4.9.1 Methods/tools 4.9.1.1 RDP 4.9.1.2 VPN 4.9.1.3 Virtual network computer (VNC) 4.9.1.4 Secure Shell (SSH) 4.9.1.5 Remote monitoring and management (RMM) 4.9.1.6 Microsoft Remote Assistance (MSRA) 4.9.1.7 Third-party tools 4.9.1.7.1 Screen-sharing software 4.9.1.7.2 Video-conferencing software 4.9.1.7.3 File transfer software 4.9.1.7.4 Desktop management software 4.9.2 Security considerations of each access method

Domain 1 Operating Systems	Domain 2 Security	Domain 3 Software Troubleshooting	Domain 4 Operational Procedures
1.10 Identify common features and tools of the macOS/desktop OS 1.10.1 Installation and uninstallation of applications 1.10.1.1 File types 1.10.1.1.1 dmg 1.10.1.1.2 pkg 1.10.1.1.3 App 1.10.1.2 App Store 1.10.1.3 Uninstallation process 1.10.2 Apple ID and corporate restrictions 1.10.3 Best practices 1.10.3.1 Backups 1.10.3.2 Antivirus 1.10.3.3 Updates/patches 1.10.4 System preferences 1.10.4.1 Displays 1.10.4.2 Networks 1.10.4.3 Printers 1.10.4.4 Scanners 1.10.4.5 Privacy 1.10.4.6 Accessibility 1.10.4.7 Time machine 1.10.5 Features 1.10.5.1 Multiple desktops 1.10.5.2 Mission Control 1.10.5.3 Keychain 1.10.5.4 Spotlight 1.10.5.5 iCloud 1.10.5.6 Gestures 1.10.5.7 Finder 1.10.5.8 Remote Disc 1.10.5.9 Dock 1.10.6 Disk Utility 1.10.7 FileVault 1.10.8 Terminal 1.10.9 Force Quit	2.10 Given a scenario, install and configure browsers and relevant security settings 2.10.1 Browser download/installation 2.10.1.1 Trusted sources 2.10.1.1.1 Hashing 2.10.1.2 Untrusted sources 2.10.2 Extensions and plug-ins 2.10.2.1 Trusted sources 2.10.2.2 Untrusted sources 2.10.3 Password managers 2.10.4 Secure connections/sites – valid certificates 2.10.5 Settings 2.10.5.1 Pop-up blocker 2.10.5.2 Clearing browsing data 2.10.5.3 Clearing cache 2.10.5.4 Private-browsing mode 2.10.5.5 Sign-in browser data synchronization 2.10.5.6 Ad blockers		

Domain 1 Operating Systems	Domain 2 Security	Domain 3 Software Troubleshooting	Domain 4 Operational Procedures
1.11 Identify common features and tools of the Linux client/desktop OS 1.11.1 Common commands 1.11.1.1 ls 1.11.1.2 pwd 1.11.1.3 mv 1.11.1.4 cp 1.11.1.5 rm 1.11.1.6 chmod 1.11.1.7 chown 1.11.1.8 su/sudo 1.11.1.9 apt-get 1.11.1.10 yum 1.11.1.11 ip 1.11.1.12 df 1.11.1.13 grep 1.11.1.14 ps 1.11.1.15 man 1.11.1.16 top 1.11.1.17 find 1.11.1.18 dig 1.11.1.19 cat 1.11.1.20 nano 1.11.2 Best practices 1.11.2.1 Backups 1.11.2.2 Antivirus 1.11.2.3 Updates/patches 1.11.3 Tools 1.11.3.1 Shell/terminal 1.11.3.2 Samba			

Lesson Plan

Approximately 35 hours of videos, labs, and projects

A+ (220-1102)

Domain 1 Lesson Plan

Approximatley 12 hours of videos, labs, and projects

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Pre-Assessment Assessment time - 00:30:00	Operating Systems: Pre-Assessment			
Lesson 1 Video time - 00:15:48 Exercise Lab time - 00:00:00 Workbook time - 00:15:00	**Windows Features** Windows 10 Editions Domains vs. Workgroups Desktop Styles and RDP RAM Support Limitations BitLocker Gpedit Upgrade Paths	1 Operating Systems 1.1 Identify basic features of Microsoft Windows editions 1.1.1 Windows 10 editions 1.1.1.1 Home 1.1.1.2 Pro 1.1.1.3 Pro for Workstations 1.1.1.4 Enterprise 1.1.2 Feature differences 1.1.2.1 Domain access vs. workgroup 1.1.2.2 Desktop styles/user interface 1.1.2.3 Availability of Remote Desktop Protocol (RDP) 1.1.2.4 Random-access memory (RAM) support limitations 1.1.2.5 BitLocker 1.1.2.6 Gpedit.msc 1.1.3 Upgrade paths 1.1.3.1 In-place upgrade	N/A	Windows 10 Editions – pg. 13 N/A Windows Feature Differences – pg. 14 N/A Upgrade Paths – pg. 15 N/A
Lesson 2 Video time - 00:16:05 Exercise Lab time - 00:24:00 Workbook time - 00:15:00	**Command Line Tools Part 1** Cd Dir Md Rmdir Drive Navigation Ipconfig and Help Ping Hostname Netstat Nslookup Chkdsk	1.2 Given a scenario, use the appropriate Microsoft command-line tool 1.2.1 Navigation 1.2.1.1 cd 1.2.1.2 dir 1.2.1.3 md 1.2.1.4 rmdir 1.2.1.5 Drive navigation inputs: 1.2.1.5.1 C: or D: or X: 1.2.2 Command-line tools 1.2.2.1 ipconfig 1.2.2.2 ping 1.2.2.3 hostname 1.2.2.4 netstat 1.2.2.5 nslookup 1.2.2.6 chkdsk 1.2.2.18 [command name] /?	Using BitLocker Cd Command Md Command Changing Drives with Commands Netstat Command Command Prompt in Elevated Mode	Navigation Commands – pg. 17 N/A Command Line Tools - Part 1 – pg. 18 N/A
Lesson 3 Video time - 00:14:29 Exercise Lab time - 00:08:00 Workbook time - 00:20:00	**Command Line Tools Part 2** Net user Net use Tracert Format Xcopy and copy Robocopy Gpupdate and Gpresult Shutdown Sfc Diskpart Pathping Winver	1.2.2.7 net user 1.2.2.8 net use 1.2.2.9 tracert 1.2.2.10 format 1.2.2.11 xcopy 1.2.2.12 copy 1.2.2.13 robocopy 1.2.2.14 gpupdate 1.2.2.15 gpresult 1.2.2.16 shutdown 1.2.2.17 Sfc 1.2.2.19 diskpart 1.2.2.20 pathping 1.2.2.21 Winver	Copy Command Diskpart Command	Command Line Tools - Part 2 – pg. 20 Folders 1101, 1102, 1103, 1104, 1105, and 1106 Command Line Tools - Part 3 – pg. 21 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 4 Video time - 00:12:24 Exercise Lab time - 00:16:00 Workbook time - 00:10:00	**Windows 10 Features and Tools Part 1** Services Startup Performance Processes and Users Event Viewer Disk Management Task Scheduler Device Manager Certificate Manager	1.3 Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS) 1.3.1 Task Manager 1.3.1.1 Services 1.3.1.2 Startup 1.3.1.3 Performance 1.3.1.4 Processes 1.3.1.5 Users 1.3.2 Microsoft Management Console (MMC) snap-in 1.3.2.1 Event Viewer (eventvwr.msc) 1.3.2.2 Disk Management (diskmgmt.msc) 1.3.2.3 Task Scheduler (taskschd.msc) 1.3.2.4 Device Manager (devmgmt.msc) 1.3.2.5 Certificate Manager (certmgr.msc)	Add Event Viewer Disk Management Task Scheduler Certificate Manager	Task Manager – pg. 23 N/A Microsoft Management Console - Part 1 – pg. 24 N/A
Lesson 5 Video time - 00:15:10 Exercise Lab time - 00:12:00 Workbook time - 00:15:00	**Windows 10 Features and Tools Part 2** Local Users and Groups Performance Monitor Group Policy Editor System Information Resource Monitor System Configuration Disk Cleanup Disk Defragment Registry Editor	1.3.2.6 Local Users and Groups (lusrmgr.msc) 1.3.2.7 Performance Monitor (perfmon.msc) 1.3.2.8 Group Policy Editor (gpedit.msc) 1.3.3 Additional tools 1.3.3.1 System Information (msinfo32.exe) 1.3.3.2 Resource Monitor (resmon.exe) 1.3.3.3 System Configuration (msconfig.exe) 1.3.3.4 Disk Cleanup (cleanmgr.exe) 1.3.3.5 Disk Defragment (dfrgui.exe) 1.3.3.6 Registry Editor (regedit.exe)	Local Users and Groups Performance Monitor Group Policy Editor	Microsoft Management Console - Part 2 – pg. 26 N/A Additional Tools – pg. 27 N/A
Lesson 6 Video time - 00:15:01 Exercise Lab time - 00:00:00 Workbook time - 00:10:00	**Control Panel Utilities Part 1** Internet Options Devices and Printers Programs and Features Network and Sharing Center System Windows Defender Firewall Mail Sound User Accounts Device Manager	1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility 1.4.1 Internet Options 1.4.2 Devices and Printers 1.4.3 Programs and Features 1.4.4 Network and Sharing Center 1.4.5 System 1.4.6 Windows Defender Firewall 1.4.7 Mail 1.4.8 Sound 1.4.9 User Accounts 1.4.10 Device Manager	N/A	Control Panel Utilities - Part 1 – pg. 29 N/A Control Panel Utilities - Part 2 – pg. 30 N/A
Lesson 7 Video time - 00:12:28 Exercise Lab time - 00:12:00 Workbook time - 00:25:00	**Control Panel Utilities Part 2** Indexing Options Administrative Tools Show Hidden Files Hide Extensions General and View Options Power Plans Hibernate Sleep, Suspend, and Standby Power Plan Settings USB Selective Suspend Ease of Access	1.4.11 Indexing Options 1.4.12 Administrative Tools 1.4.13 File Explorer options 1.4.13.1 Show hidden files 1.4.13.2 Hide extensions 1.4.13.3 General options 1.4.13.4 View options 1.4.14 Power options 1.4.14.1 Hibernate 1.4.14.2 Power plans 1.4.14.3 Sleep/suspend 1.4.14.4 Standby 1.4.14.5 Choose what closing the lid does 1.4.14.6 Turn on fast startup 1.4.14.7 Universal Serial Bus (USB) selective suspend 1.4.15 Ease of Access	Index Options General and View Options Power Plan Settings	Indexing and Administrative Tools – pg. 32 N/A File Explorer Options – pg. 33 N/A Power Options – pg. 34 N/A Ease of Access – pg. 35 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 8 Video time - 00:13:54 Exercise Lab time - 00:04:00 Workbook time - 00:10:00	**Windows Settings** Time and Language Update and Security Personalization Apps Privacy System Settings Devices Network and Internet Gaming Accounts	1.5 Given a scenario, use the appropriate Windows settings 1.5.1 Time & Language 1.5.2 Update & Security 1.5.3 Personalization 1.5.4 Apps 1.5.5 Privacy 1.5.6 System 1.5.7 Devices 1.5.8 Network & Internet 1.5.9 Gaming 1.5.10 Accounts	Time and Language Settings	Windows Settings - Part 1 – pg. 37 N/A Windows Settings - Part 2 – pg. 38 N/A
Lesson 9 Video time - 00:11:31 Exercise Lab time - 00:16:00 Workbook time - 00:15:00	**Client Networking Features Part 1** Shared Resources and File Servers Printers Mapped Drives Firewall Restrictions and Exceptions Firewall Configuration IP Addressing Schemes DNS Subnet Mask	1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop 1.6.1 Workgroup vs. domain setup 1.6.1.1 Shared resources 1.6.1.2 Printers 1.6.1.3 File servers 1.6.1.4 Mapped drives 1.6.2 Local OS firewall settings 1.6.2.1 Application restrictions and exceptions 1.6.2.2 Configuration 1.6.3 Client network configuration 1.6.3.1 Internet Protocol (IP) addressing scheme 1.6.3.2 Domain Name System (DNS) 1.6.3.3 Subnet mask	Shared Resources Sharing Printers Firewall Configuration DNS	Workgroup vs. Domain Setup – pg. 40 Student folder Local OS Firewall Settings – pg. 41 N/A Client Network Configuration - Part 1 – pg. 42 N/A
Lesson 10 Video time - 00:12:23 Exercise Lab time - 00:04:00 Workbook time - 00:15:00	**Client Networking Features Part 2** Gateway and Addressing Types VPN Wireless Connection Wired Connection WWAN Proxy Settings Public vs. Private Networks File Explorer Navigation Metered Connections and Limitations	1.6.3.4 Gateway 1.6.3.5 Static vs. dynamic 1.6.4 Establish network connections 1.6.4.1 Virtual private network (VPN) 1.6.4.2 Wireless 1.6.4.3 Wired 1.6.4.4 Wireless wide area network (WWAN) 1.6.5 Proxy settings 1.6.6 Public network vs. private network 1.6.7 File Explorer navigation – network paths 1.6.8 Metered connections and limitations	Add a VPN	Client Network Configuration - Part 2 – pg. 44 N/A Establishing Network Connections – pg. 45 N/A Other Client Network Features – pg. 46 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 11 Video time - 00:12:21 Exercise Lab time - 00:00:00 Workbook time - 00:20:00	**App Installs and Configurations** 32-Bit vs. 64-Bit Dependencies Graphics Card Types Video and Physical RAM CPU and Storage Requirements External Hardware Tokens Application to OS Compatibility 32-Bit vs. 64-Bit OS Physical vs. Downloadable Media ISO Mountable New App Considerations	1.7 Given a scenario, apply application installation and configuration concepts 1.7.1 System requirements for applications 1.7.1.1 32-bit vs. 64-bit dependent application requirements 1.7.1.2 Dedicated graphics card vs. integrated 1.7.1.3 Video random-access memory (VRAM) requirements 1.7.1.4 RAM requirements 1.7.1.5 Central processing unit (CPU) requirements 1.7.1.6 External hardware tokens 1.7.1.7 Storage requirements 1.7.2 OS requirements for applications 1.7.2.1 Application to OS compatibility 1.7.2.2 32-bit vs. 64-bit OS 1.7.3 Distribution methods 1.7.3.1 Physical media vs. downloadable 1.7.3.2 ISO mountable 1.7.4 Other considerations for new applications 1.7.4.1 Impact to device 1.7.4.2 Impact to network 1.7.4.3 Impact to operation 1.7.4.4 Impact to business	N/A	App System Requirements – pg. 48 N/A OS Requirements for Apps and Distribution Methods – pg. 49 N/A App Impact Considerations – pg. 50 N/A
Lesson 12 Video time - 00:13:55 Exercise Lab time - 00:04:00 Workbook time - 00:20:00	**OS Types and Their Purposes** Windows Linux macOS Chrome OS iPadOS iOS Android NTFS FAT32 and exFAT Ext3 and Ext4 APFS EOL and Update Limitations Compatibility Concerns Between OSs	1.8 Explain common OS types and their purposes 1.8.1 Workstation OSs 1.8.1.1 Windows 1.8.1.2 Linux 1.8.1.3 macOS 1.8.1.4 Chrome OS 1.8.2 Cell phone/tablet OSs 1.8.2.1 iPadOS 1.8.2.2 iOS 1.8.2.3 Android 1.8.3 Various filesystem types 1.8.3.1 New Technology File System (NTFS) 1.8.3.2 File Allocation Table 32 (FAT32) 1.8.3.3 Third extended filesystem (ext3) 1.8.3.4 Fourth extended filesystem (ext4) 1.8.3.5 Apple File System (APFS) 1.8.3.6 Extensible File Allocation Table (exFAT) 1.8.4 Vendor life-cycle limitations 1.8.4.1 End-of-life (EOL) 1.8.4.2 Update limitations 1.8.5 Compatibility concerns between OSs	Mac File Systems	Workstation Operating Systems – pg. 52 N/A Cell Phone and Tablet Operating Systems – pg. 53 N/A Types of File Systems – pg. 54 N/A Vendor and Compatibility Issues – pg. 55 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 13 Video time - 00:18:55 Exercise Lab time - 00:08:00 Workbook time - 00:30:00	**OS Installations** USB, Optical, SSD, External Boot Network, Internet-Based Boot Internal Hard Drive Partition Recovery, Repair, Remote Installations Types of Image Deployments Partitioning Drive Format Backup Files and User Preferences App and Driver Support Hardware Compatibility Feature Updates	1.9 Given a scenario, perform OS installations and upgrades in a diverse OS environment 1.9.1 Boot methods 1.9.1.1 USB 1.9.1.2 Optical media 1.9.1.3 Network 1.9.1.4 Solid-state/flash drives 1.9.1.5 Internet-based 1.9.1.6 External/hot-swappable drive 1.9.1.7 Internal hard drive (partition) 1.9.2 Types of installations 1.9.2.1 Upgrade 1.9.2.2 Recovery partition 1.9.2.3 Clean install 1.9.2.4 Image deployment 1.9.2.5 Repair installation 1.9.2.6 Remote network installation 1.9.2.7 Other considerations 1.9.2.7.1 Third-party drivers 1.9.3 Partitioning 1.9.3.1 GUID [globally unique identifier] Partition Table (GPT) 1.9.3.2 Master boot record (MBR) 1.9.4 Drive format 1.9.5 Upgrade considerations 1.9.5.1 Backup files and user preferences 1.9.5.2 Application and driver support/backward compatibility 1.9.5.3 Hardware compatibility 1.9.6 Feature updates 1.9.6.1Product life cycle	Installing Windows Formatting a Drive	OS Installations – pg. 57 N/A OS Upgrades – pg. 58 N/A Drive Partitioning and Formats – pg. 59 N/A Upgrades and Updates – pg. 60 N/A
Lesson 14 Video time - 00:14:53 Exercise Lab time - 00:04:00 Workbook time - 00:25:00	**macOS Tools and Features Part 1** App Installs Apple IDs Backups Antivirus Updates and Patches Displays Networks Printers and Scanners Privacy Settings Accessibility Time Machine Multiple Desktops, Mission Control Keychain	1.10 Identify common features and tools of the macOS/desktop OS 1.10.1 Installation and uninstallation of applications 1.10.1.1 File types 1.10.1.1.1 dmg 1.10.1.1.2 pkg 1.10.1.1.3 App 1.10.1.2 App Store 1.10.1.3 Uninstallation process 1.10.2 Apple ID and corporate restrictions 1.10.3 Best practices 1.10.3.1 Backups 1.10.3.2 Antivirus 1.10.3.3 Updates/patches 1.10.4 System preferences 1.10.4.1 Displays 1.10.4.1 Networks 1.10.4.3 Printers 1.10.4.4 Scanners 1.10.4.5 Privacy 1.10.4.6 Accessibility 1.10.4.7 Time machine 1.10.5 Features 1.10.5.1 Multiple desktops 1.10.5.2 Mission Control 1.10.5.3 Keychain	XProtect	Mac App Installs – pg. 62 N/A Apple IDs and Best Practices – pg. 63 N/A Mac System Preferences – pg. 64 N/A mac OS Features - Part 1 – pg. 65 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 15 Video time - 00:12:19 Exercise Lab time - 00:04:00 Workbook time - 00:10:00	**macOS Tools and Features Part 2** Spotlight iCloud Gestures Finder, Remote Disc Dock Disk Utility FileVault Terminal Force Quit	1.10.5.4 Spotlight 1.10.5.5 iCloud 1.10.5.6 Gestures 1.10.5.7 Finder 1.10.5.8 Remote Disc 1.10.5.9 Dock 1.10.6 Disk Utility 1.10.7 FileVault 1.10.8 Terminal 1.10.9 Force Quit	Force Quit	mac OS Features - Part 2 – pg. 67 N/A mac OS Features - Part 3 – pg. 68 N/A
Lesson 16 Video time - 00:13:41 Exercise Lab time - 00:00:00 Workbook time - 00:10:00	**Linux Tools and Features Part 1** Ls and Man Pwd Mv, Cp, Rm Chmod Chown, Su/sudo Apt-get, Yum Ip Df Grep, Find	1.11 Identify common features and tools of the Linux client/desktop OS 1.11.1 Common commands 1.11.1.1 ls 1.11.1.2 pwd 1.11.1.3 mv 1.11.1.4 cp 1.11.1.5 rm 1.11.1.6 chmod 1.11.1.7 chown 1.11.1.8 su/sudo 1.11.1.9 apt-get 1.11.1.10 yum 1.11.1.11 ip 1.11.1.12 df 1.11.1.13 grep 1.11.1.15 man 1.11.1.17 find	N/A	Linux Commands - Part 1 – pg. 70 N/A Linux Commands - Part 2 – pg. 71 N/A
Lesson 17 Video time - 00:13:36 Exercise Lab time - 00:00:00 Workbook time - 00:10:00	**Linux Tools and Features Part 2** Ps Top Dig Cat, Nano Linux Backups Linux Antivirus Linux Updates/Patches Shell/Terminal	1.11.1.14 ps 1.11.1.16 top 1.11.1.18 dig 1.11.1.19 cat 1.11.1.20 nano 1.11.2 Best practices 1.11.2.1 Backups 1.11.2.2 Antivirus 1.11.2.3 Updates/patches 1.11.3 Tools 1.11.3.1 Shell/terminal 1.11.3.2 Samba	N/A	Linux Commands - Part 3 – pg. 73 N/A Linux Best Practices – pg. 74 N/A
Post-Assessment Assessment time - 01:00:00	Operating Systems: Post-Assessment			

Domain 2 Lesson Plan

Approximately 10.5 hours of videos, labs, and projects

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Pre-Assessment Assessment time - 00:30:00	Security: Pre-Assessment			
Lesson 1 Video time - 00:13:45 Exercise Lab time - 00:15:00 Workbook time - 00:15:00	**Security Measures Part 1** Access Control Vestibule Badge Reader Video Surveillance Alarm Systems Motion Sensors Door Locks Equipment Locks Guards Bollards and Fences Key Fobs Smart Cards Keys Biometrics Lighting Magnetometers	2.1 Summarize various security measures and their purposes 2.1.1 Physical security 2.1.1.1 Access control vestibule 2.1.1.2 Badge reader 2.1.1.3 Video surveillance 2.1.1.4 Alarm systems 2.1.1.5 Motion sensors 2.1.1.6 Door locks 2.1.1.7 Equipment locks 2.1.1.8 Guards 2.1.1.9 Bollards 2.1.1.10 Fences 2.1.2 Physical security for staff 2.1.2.1 Key fobs 2.1.2.2 Smart cards 2.1.2.3 Keys 2.1.2.4 Biometrics 2.1.2.4.1 Retina scanner 2.1.2.4.2 Fingerprint scanner 2.1.2.4.3 Palmprint scanner 2.1.2.5 Lighting 2.1.2.6 Magnetometers	N/A	Physical Security Measures – pg. 76 N/A Physical Staff Security – pg. 77 N/A
Lesson 2 Video time - 00:20:52 Exercise Lab time - 00:20:00 Workbook time - 00:20:00	**Security Measures Part 2** Principle of Least Privilege Access Control Lists Multifactor Authentication Email Hard Token Soft Token SMS and Voice Call Authenticator Application Mobile Device Management Logon Script Domain Group Policy and Updates Organizational Units Home Folder Folder Redirection Security Groups	2.1.3 Logical security 2.1.3.1 Principle of least privilege 2.1.3.2 Access control lists (ACLs) 2.1.3.3 Multifactor authentication (MFA) 2.1.3.4 Email 2.1.3.5 Hard token 2.1.3.6 Soft token 2.1.3.7 Short message service (SMS) 2.1.3.8 Voice call 2.1.3.9 Authenticator application 2.1.4 Mobile device management (MDM) 2.1.5 Active Directory 2.1.5.1 Logon script 2.1.5.2 Domain 2.1.5.3 Group Policy/updates 2.1.5.4 Organizational units 2.1.5.5 Home folder 2.1.5.6 Folder redirection 2.1.5.7 Security groups	Login Script Group Policy Management Connecting a Home Folder Folder Redirection Creating a Security Group	Logical Security – pg. 79 N/A Mobile Device Management – pg. 80 N/A Active Directory – pg. 81 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 3 Video time - 00:07:14 Exercise Lab time - 00:00:00 Workbook time - 00:15:00	**Wireless Security Protocols** WPA2 and AES WPA3 and TKIP RADIUS and TACACS+ Kerberos Multifactor	2.2 Compare and contrast wireless security protocols and authentication methods 2.2.1 Protocols and encryption 2.2.1.1 Wi-Fi Protected Access 2 (WPA2) 2.2.1.2 WPA3 2.2.1.3 Temporal Key Integrity Protocol (TKIP) 2.2.1.4 Advanced Encryption Standard (AES) 2.2.2 Authentication 2.2.2.1 Remote Authentication Dial-In User Service (RADIUS) 2.2.2.2 Terminal Access Controller Access-Control System (TACACS+) 2.2.2.3 Kerberos 2.2.2.4 Multifactor	N/A	Wireless Security Protocols and Encryption – pg. 83 N/A Authentication Methods – pg. 84 N/A
Lesson 4 Video time - 00:16:05 Exercise Lab time - 00:04:00 Workbook time - 00:20:00	**Malware** Trojan Rootkit Virus Spyware Ransomware Keylogger Boot Sector Virus Cryptominers Recovery Mode Antivirus and Antimalware Software Firewalls Anti-Phishing Training Educating Users on Common Threats OS Reinsatallaton	2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods 2.3.1 Malware 2.3.1.1 Trojan 2.3.1.2 Rootkit 2.3.1.3 Virus 2.3.1.4 Spyware 2.3.1.5 Ransomware 2.3.1.6 Keylogger 2.3.1.7 Boot sector virus 2.3.1.8 Cryptominers 2.3.2 Tools and methods 2.3.2.1 Recovery mode 2.3.2.2 Antivirus 2.3.2.3 Anitmalware 2.3.2.4 Software firewalls 2.3.2.5 Anti-phishing training 2.3.2.6 User education regarding common threats 2.3.2.7 OS reinstallation	Windows Defender Firewall	Viruses – pg. 86 N/A Other Malware – pg. 87 N/A Malware Removal – pg. 88 N/A Malware Prevention – pg. 89 N/A
Lesson 5 Video time - 00:09:04 Exercise Lab time - 00:00:00 Workbook time - 00:10:00	**Social Engineering Part 1** Phishing Vishing Shoulder Surfing Whaling Tailgating Impersonation Dumpster Diving Evil Twin	2.4 Explain common social-engineering attacks, threats, and vulnerabilities 2.4.1 Social engineering 2.4.1.1 Phishing 2.4.1.2 Vishing 2.4.1.3 Shoulder surfing 2.4.1.4 Whaling 2.4.1.5 Tailgating 2.4.1.6 Impersonation 2.4.1.7 Dumpster diving 2.4.1.8 Evil twin 2.4.2 Threats	N/A	Forms of Phishing – pg. 91 N/A Other Social Engineering – pg. 92 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 6 Video time - 00:12:41 Exercise Lab time - 00:00:00 Workbook time - 00:20:00	**Social Engineering Part 2** DoS and DDoS Zero-Day Attack Spoofing On-Path Attack Brute-Force Attack Dictionary Attack Insider Threat SQL Injection Non-Compliant and Unpatched Systems Unprotected Systems EOL Operating Systems BYOD	2.4.2.1 Distributed denial of service (DDoS) 2.4.2.2 Denial of Service (DoS) 2.4.2.3 Zero-day attack 2.4.2.4 Spoofing 2.4.2.5 On-path attack 2.4.2.6 Brute-force attack 2.4.2.7 Dictionary attack 2.4.2.8 Insider threat 2.4.2.9 Structured Query Language (SQL) injection 2.4.3 Vulnerabilities 2.4.3.1 Non-compliant systems 2.4.3.2 Unpatched systems 2.4.3.3 Unprotected systems (missing antivirus/missing firewall) 2.4.3.4 EOL OSs 2.4.3.5 Bring your own device (BYOD)	N/A	Network and Device Attacks – pg. 94 N/A Other Threats – pg. 95 N/A Vulnerabilities – pg. 96 N/A
Lesson 7 Video time - 00:11:24 Exercise Lab time - 00:12:00 Workbook time - 00:10:00	**Windows Security Settings Part 1** Activate Defender Updated Definitions Activate Firewall Port Security Application Security Local vs. Microsoft Account Standard vs. Administrator Account Guest User Power User	2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS 2.5.1 Defender Antivirus 2.5.1.1 Activate/deactivate 2.5.1.2 Updated definitions 2.5.2 Firewall 2.5.2.1 Activate/deactivate 2.5.2.2 Port security 2.5.2.3 Application security 2.5.3 Users and groups 2.5.3.1 Local vs. Microsoft account 2.5.3.2 Standard account 2.5.3.3 Administrator 2.5.3.4 Guest user 2.5.3.3 Power user	Deactivate a Firewall Port Security Application Security	Defender Antivirus and Firewall – pg. 98 N/A Users and Groups – pg. 99 N/A
Lesson 8 Video time - 00:13:19 Exercise Lab time - 00:12:00 Workbook time - 00:25:00	**Windows Security Settings Part 2** Username, Password, PIN Fingerprint and Facial Recognition SSO File and Folder Attributes Inheritance UAC BitLocker and BitLocker To Go EFS	2.5.4 Login OS options 2.5.4.1 Username and password 2.5.4.2 Personal identification number (PIN) 2.5.4.3 Fingerprint 2.5.4.4 Facial recognition 2.5.4.5 Single sign-on (SSO) 2.5.5 NTFS vs. share permissions 2.5.5.1 File and folder attributes 2.5.5.2 Inheritance 2.5.6 Run as administrator vs. standard user 2.5.6.1 User Account Control (UAC) 2.5.7 BitLocker 2.5.8 BitLocker To Go 2.5.9 Encrypting File System (EFS)	NTFS Folder Permissions Inheritance BitLocker To Go	Login OS Options – pg. 101 N/A NTFS vs. Share Permissions – pg. 102 Signature Files folder User Account Control – pg. 103 N/A Data Encryption Features – pg. 104 onlinescripts folder

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 9 Video time - 00:17:47 Exercise Lab time - 00:36:00 Workbook time - 00:30:00	**Workstation Best Practices** Data-at-Rest Password Complexity Requirements Expiration Requirements BIOS/UEFI Passwords Screensaver Locks Signing Off when not in Use Secure Hardware, PII, and Passwords Restrict User Permissions Restrict Sign-In Times Disable Guest Account Use Failed Attempts Lockout Use Timeout/Screen Lock Change Default Administrator Account Disable AutoRun Disable AutoPlay	2.6 Given a scenario, configure a workstation to meet best practices for security 2.6.1 Data-at-rest encryption 2.6.2 Password best practices 2.6.2.1 Complexity requirements 2.6.2.1.1 Length 2.6.2.1.2 Character types 2.6.2.2 Expiration requirements 2.6.2.3 Basic input/output system (BIOS)/ Unified Extensible Firmware Interface (UEFI) passwords 2.6.3 End-user best practices 2.6.3.1 Use screensaver locks 2.6.3.2 Log off when not in use 2.6.3.3 Secure/protect critical hardware (e.g., laptops) 2.6.3.4 Secure personally identifiable information (PII) and passwords 2.6.4 Account management 2.6.4.1 Restrict user permissions 2.6.4.2 Restrict login times 2.6.4.3 Disable guest account 2.6.4.4 Use failed attempts lockout 2.6.4.5 Use timeout/screen lock 2.6.5 Change default administrator's user account/password 2.6.6 Disable AutoRun 2.6.7 Disable AutoPlay	Password Complexity Requirements Locking a Device Restricting User Permissions Disabling Accounts Lockout Policies Screen Lock Renaming Accounts Disabling AutoRun Disabling AutoPlay	Data Storage and Password Best Practices – pg. 106 N/A End-User Best Practices – pg. 107 N/A Account Mangement – pg. 108 N/A
Lesson 10 Video time - 00:16:02 Exercise Lab time - 00:08:00 Workbook time - 00:25:00	**Securing Mobile Devices** Facial Recognition PIN Codes and Swipes Fingerpint and Patterns Remote Wipes Locator Applications OS Updates Device Encryption Remote Backup Applications Failed Login Attempt Restrictions Antivirus/Antimalware Firewalls BYOD vs. Corporate-Owned Devices Profile Security Requirements IoT	2.7 Explain common methods for securing mobile and embedded devices 2.7.1 Screen locks 2.7.1.1 Facial recognition 2.7.1.2 PIN codes 2.7.1.3 Fingerprint 2.7.1.4 Pattern 2.7.1.5 Swipe 2.7.2 Remote wipes 2.7.3 Locator applications 2.7.4 OS updates 2.7.5 Device encryption 2.7.6 Remote backup applications 2.7.7 Failed login attempts restrictions 2.7.8 Antivirus/anti-malware 2.7.9 Firewalls 2.7.10 Policies and procedures 2.7.10.1 BYOD vs. corporate owned 2.7.10.2 Profile security requirements 2.7.11 Internet of Things (IoT)	Setting a PIN Creating Compliance Policies	Screen Locks – pg. 110 N/A Mobile Device Security – pg. 111 N/A Policies – pg. 112 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 11 Video time - 00:11:53 Exercise Lab time - 00:04:00 Workbook time - 00:25:00	**Data Destruction and Disposal and SOHO Network Security Settings Part 1** Drilling Shredding and Incinerating Degaussing Erasing and Wiping Low-Level and Standard Formatting Vendors and Certificates of Destruction Change Default Passwords IP Filtering Firmware Updates Content Filtering Physical Placement DHCP Reservations Static WAN UPnP Screened Subnet	2.8 Given a scenario, use common data destruction and disposal methods 2.8.1 Physical destruction 2.8.1.1 Drilling 2.8.1.2 Shredding 2.8.1.3 Degaussing 2.8.1.4 Incinerating 2.8.2 Recycling or repurposing best practices 2.8.2.1 Erasing/wiping 2.8.2.2 Low-level formatting 2.8.2.3 Standard formatting 2.8.3 Outsourcing concepts 2.8.3.1 Third-party vendor 2.8.3.2 Certification of destruction/recycling 2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks 2.9.1 Home router settings 2.9.1.1 Change default passwords 2.9.1.2 IP filtering 2.9.1.3 Firmware updates 2.9.1.4 Content filtering 2.9.1.5 Physical placement/secure locations 2.9.1.6 Dynamic Host Configuration Protocol (DHCP) reservations 2.9.1.7 Static wide-area network (WAN) IP 2.9.1.8 Universal Plug and Play (UPnP) 2.9.1.9 Screened subnet	Content Filtering	Data Destruction and Repurposing – pg. 114 N/A Router and WAP Settings - Part 1 – pg. 115 N/A Router and WAP Settings - Part 2 – pg. 116 N/A
Lesson 12 Video time - 00:10:13 Exercise Lab time - 00:12:00 Workbook time - 00:10:00	**SOHO Network Security Settings Part 2** Changing the SSID Disabling SSID Broadcast Encryption Settings Disabling Guest Access Changing Channels Disabling Unused Ports Port Forwarding/Mapping	2.9.2 Wireless specific 2.9.2.1 Changing the service set identifier (SSID) 2.9.2.2 Disabling SSID broadcast 2.9.2.3 Encryption settings 2.9.2.4 Disabling guest access 2.9.2.5 Changing channels 2.9.3 Firewall settings 2.9.3.1 Disabling unused ports 2.9.3.2 Port forwarding/mapping	Changing an SSID Protocols and Encryption Port Forwarding	Wireless Network Security – pg. 118 N/A
Lesson 13 Video time - 00:12:18 Exercise Lab time - 00:04:00 Workbook time - 00:20:00	**Install and Configure Browsers** Browser Download and Installation Extensions and Plug-Ins Password Managers Secure Connections and Certificates Pop-Up Blockers Clearing Browsing Data and Cache Private Browsing Mode Sign-In Data Synchronization Ad Blockers	2.10 Given a scenario, install and configure browsers and relevant security settings 2.10.1 Browser download/installation 2.10.1.1 Trusted sources 2.10.1.1.1 Hashing 2.10.1.2 Untrusted sources 2.10.2 Extensions and plug-ins 2.10.2.1 Trusted sources 2.10.2.2 Untrusted sources 2.10.3 Password managers 2.10.4 Secure connections/sites – valid certificates 2.10.5 Settings 2.10.5.1 Pop-up blocker 2.10.5.2 Clearing browsing data 2.10.5.3 Clearing cache 2.10.5.4 Private-browsing mode 2.10.5.5 Sign-in browser data synchronization 2.10.5.6 Ad blockers	Pop-Up Blocker	Web Browsers – pg. 120 N/A Web Browser Settings – pg. 121 N/A
Post-Assessment Assessment time - 01:00:00	Security: Post-Assessment			

Domain 3 Lesson Plan

Approximately 6 hours of videos, labs, and projects

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Pre-Assessment Assessment time - 00:30:00	Software Troubleshooting: Pre-Assessment			
Lesson 1 Video time - 00:20:58 Exercise Lab time - 00:20:00 Workbook time - 00:20:00	**Common Windows OS Problems Part 1** BSOD Sluggish Performance Boot Problems Frequent Shutdowns Services not Starting Applications Crashing Low Memory Warnings USB Controller Resource Warnings System Instability No OS Found Slow Profile Load Time Drift	3.1 Given a scenario, troubleshoot common Windows OS problems 3.1.1 Common symptoms 3.1.1.1 Blue screen of death (BSOD) 3.1.1.2 Sluggish performance 3.1.1.3 Boot problems 3.1.1.4 Frequent shutdowns 3.1.1.5 Services not starting 3.1.1.6 Applications crashing 3.1.1.7 Low memory warnings 3.1.1.8 USB controller resource warnings 3.1.1.9 System instability 3.1.1.10 No OS found 3.1.1.11 Slow profile load 3.1.1.12 Time drift	Boot Logging Errors with Service Events Service Sign-In Accounts Crashing App Troubleshooting Page Files	Windows Issues - Part 1 – pg. 123 N/A Windows Issues - Part 2 – pg. 124 N/A
Lesson 2 Video time - 00:15:32 Exercise Lab time - 00:20:00 Workbook time - 00:15:00	**Common Windows OS Problems Part 2** Reboot Restart Services App Uninstalls and Updates Add Resources Verify Requirements System File Check Repair Windows Restore Reimage Roll Back Updates Rebuild Windows Profiles	3.1.2 Common troubleshooting steps 3.1.2.1 Reboot 3.1.2.2 Restart services 3.1.2.3 Uninstall/reinstall/update applications 3.1.2.4 Add resources 3.1.2.5 Verify requirements 3.1.2.6 System file check 3.1.2.7 Repair Windows 3.1.2.8 Restore 3.1.2.9 Reimage 3.1.2.10 Roll back updates 3.1.2.11 Rebuild Windows profiles	Restarting a Service Adding Resources to a VM Creating a Restore Point Using a Restore Point Reimage	Windows Troubleshooting - Part 1 – pg. 126 N/A Windows Troubleshooting - Part 1 – pg. 127 N/A
Lesson 3 Video time - 00:12:10 Exercise Lab time - 00:00:00 Workbook time - 00:15:00	**Common PC Security Issues** No Network Access Desktop Alerts False Antivirus Alerts Altered System or Personal Files Unwanted Notifications OS Update Failures Random or Frequent Pop-Ups Certificate Warnings Redirection	3.2 Given a scenario, troubleshoot common personal computer (PC) security issues 3.2.1 Common symptoms 3.2.1.1 Unable to access the network 3.2.1.2 Desktop alerts 3.2.1.3 False alerts regarding antivirus protection 3.2.1.4 Altered system or personal files 3.2.1.4.1 Missing/renamed files 3.2.1.5 Unwanted notifications within the OS 3.2.1.6 OS update failures 3.2.2 Browser-related symptoms 3.2.2.1 Random/frequent pop-ups 3.2.2.2 Certificate warnings 3.2.2.3 Redirection	N/A	PC Security Issues – pg. 129 N/A Browser Security Issues – pg. 130 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 4 Video time - 00:10:36 Exercise Lab time - 00:12:00 Workbook time - 00:15:00	**Malware Removal Best Practices** Investigate and Verify Malware Quarantine Infected Systems Disable System Restore Update Antimalware Software Scanning and Removal Techniques Schedule Scans and Run Updates Create a System Restore Point Educate the End User	3.3 Given a scenario, use best practice procedures for malware removal 3.3.1 1. Investigate and verify malware symptoms 3.3.2 2. Quarantine infected systems 3.3.3 3. Disable System Restore in Windows 3.3.4 Remediate infected systems 3.3.4.1 Update anti-malware software 3.3.4.2 Scanning and removal techniques (e.g., safe mode, preinstallation environment) 3.3.5 Schedule scans and run updates 3.3.6 Enable System Restore and create a restore point in Windows 3.3.7 Educate the end user	Disable System Restore in Windows Schedule Regular Scans Create a System Restore Point	Malware Removal - First Steps – pg. 132 N/A Remediating Systems – pg. 133 N/A
Lesson 5 Video time - 00:13:03 Exercise Lab time - 00:12:00 Workbook time - 00:15:00	**Common Mobile OS and App Issues** Application Fails to Launch Application Fails to Close Application Fails to Update Slow to Respond OS Fails to Update Battery Life Issues Random Reboots Connectivity Issues Screen does not Autorotate	3.4 Given a scenario, troubleshoot common mobile OS and application issues 3.4.1 Common symptoms 3.4.1.1 Application fails to launch 3.4.1.2 Application fails to close/crashes 3.4.1.3 Application fails to update 3.4.1.4 Slow to respond 3.4.1.5 OS fails to update 3.4.1.6 Battery life issues 3.4.1.7 Randomly reboots 3.4.1.8 Connectivity issues 3.4.1.8.1 Bluetooth 3.4.1.8.2 WiFi 3.4.1.8.3 Near-field communication (NFC) 3.4.1.8.4 AirDrop 3.4.1.9 Screen does not autorotate	Clear a Cache App Performance Portrait Orientation Lock	Mobile OS and App Issues - Part 1 – pg. 135 N/A Mobile OS and App Issues - Part 1 – pg. 136 N/A
Lesson 6 Video time - 00:17:36 Exercise Lab time - 00:08:00 Workbook time - 00:15:00	**Common Mobile OS and App Security Issues** APK Source Developer Mode Root Access/Jailbreak Bootleg/Malicious App High Network Traffic Sluggish Response Time Data-Usage Limit Notification Limited Internet Connectivity No Internet Connectivity High Number of Ads Fake Security Warnings Unexpected Application Behavior Leaked Personal Files/Data	3.5 Given a scenario, troubleshoot common mobile OS and application security issues 3.5.1 Security concerns 3.5.1.1 Android package (APK) source 3.5.1.2 Developer mode 3.5.1.3 Root access/jailbreak 3.5.1.4 Bootleg/malicious application 3.5.1.4.1 Application spoofing 3.5.2 Common symptoms 3.5.2.1 High network traffic 3.5.2.2 Sluggish response time 3.5.2.3 Data-usage limit notification 3.5.2.4 Limited internet connectivity 3.5.2.5 No internet connectivity 3.5.2.6 High number of ads 3.5.2.7 Fake security warnings 3.5.2.8 Unexpected application behavior 3.5.2.9 Leaked personal files/data	Developer Mode Block Rooted Devices	Mobile OS and App Security Concerns – pg. 138 N/A Mobile OS and App Security Issues – pg. 139 N/A
Post-Assessment **Assessment time - 01:00:00**	Software Troubleshooting: Post-Assessment			

Domain 4 Lesson Plan

Approximately 6.5 hours of videos, labs, and projects

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Pre-Assessment Assessment time - 00:30:00	Operational Procedures: Pre-Assessment			
Lesson 1 Video time - 00:22:55 Exercise Lab time - 00:00:00 Workbook time - 00:30:00	**Documentation Best Practices Part 1** User Information on Ticketing Systems Device Information Problem, Category, and Severity Escalation Levels Clear and Concise Communication Inventory List Database System Asset Tags and IDs Procurement Life Cycle Warranty and Licensing Assigned Users AUP Network Topology Diagram Regulatory Compliance Requirements Incident Reports Standard Operating Procedures New User Setup Checklist End User Termination Checklist Knowledge Base/Articles	4.1 Given a scenario, implement best practices associated with documentation and support systems information management 4.1.1 Ticketing systems 4.1.1.1 User information 4.1.1.2 Device information 4.1.1.3 Description of problems 4.1.1.4 Categories 4.1.1.5 Severity 4.1.1.6 Escalation levels 4.1.1.7 Clear, concise written communication 4.1.1.7.1 Problem description 4.1.1.7.2 Progress notes 4.1.1.7.3 Problem resolution 4.1.2 Asset management 4.1.2.1 Inventory lists 4.1.2.2 Database system 4.1.2.3 Asset tags and IDs 4.1.2.4 Procurement life cycle 4.1.2.5 Warranty and licensing 4.1.2.6 Assigned users 4.1.3 Types of documents 4.1.3.1 Acceptable use policy (AUP) 4.1.3.2 Network topology diagram 4.1.3.3 Regulatory compliance requirements 4.1.3.3.1 Splash screens 4.1.3.4 Incident reports 4.1.3.5 Standard operating procedures 4.1.3.5.1 Procedures for custom installation of software package 4.1.3.6 New user setup checklist 4.1.3.7 End user termination checklist 4.1.4 Knowledge base/articles	N/A	Ticketing Systems – pg. 141 N/A Asset Management – pg. 142 N/A Documents and Knowledge Bases – pg. 143 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 2 Video time - 00:18:02 Exercise Lab time - 00:04:00 Workbook time - 00:25:00	**Change Management Best Practices** Rollback Plan Sandbox Testing and Responsible Staff Request Forms Purpose and Scope of Change Time and Impact of Change Risk Analysis Change Board Approvals End-User Acceptance Backup and Recovery Full Incremental Differential Synthetic Backup Testing On-Site vs. Off-Site and 3-2-1 GFS	4.2 Explain basic change-management best practices 4.2.1 Documented business processes 4.2.1.1 Rollback plan 4.2.1.2 Sandbox testing 4.2.1.3 Responsible staff member 4.2.2 Change management 4.2.2.1 Request forms 4.2.2.2 Purpose of the change 4.2.2.3 Scope of the change 4.2.2.4 Date and time of the change 4.2.2.5 Affected systems/impact 4.2.2.6 Risk analysis 4.2.2.6.1 Risk level 4.2.2.7 Change board approvals 4.2.2.8 End-user acceptance 4.3 Given a scenario, implement workstation backup and recovery methods 4.3.1 Backup and recovery 4.3.1.1 Full 4.3.1.2 Incremental 4.3.1.3 Differential 4.3.1.4 Synthetic 4.3.2 Backup testing 4.3.2.1 Frequency 4.3.3 Backup rotation schemes 4.3.3.1 On-site vs. off-site 4.3.3.2 Grandfather-Father-Son (GFS) 4.3.3.3 3-2-1 backup rule	Testing a Backup	Change Management – pg. 145 N/A Change Request Forms – pg. 146 N/A Backups – pg. 147 N/A
Lesson 3 Video time - 00:18:13 Exercise Lab time - 00:00:00 Workbook time - 00:25:00	**Common Safety Procedures** ESD Straps ESD Mats Equipment Grounding Proper Power Handling Components and Antistatic Bags Compliance with Government Regulations Disconnect Power Before Repairing Lifting Techniques, Fire Safety Protecting the Eyes, Nose, and Mouth Environmental Impacts and Controls Proper Battery Disposal Proper Toner Disposal Proper Disposal of Other Devices Equipment Location and Placement Dust, Compressed Air, and Vacuums Battery Backup Surge Suppressor	4.4 Given a scenario, use common safety procedures 4.4.1 Electrostatic discharge (ESD) straps 4.4.2 ESD mats 4.4.3 Equipment grounding 4.4.4 Proper power handling 4.4.5 Proper component handling and storage 4.4.6 Antistatic bags 4.4.7 Compliance with government regulations 4.4.8 Personal safety 4.4.8.1 Disconnect power before repairing PC 4.4.8.2 Lifting techniques 4.4.8.3 Electrical fire safety 4.4.8.4 Safety goggles 4.4.8.5 Air filtration mask 4.5 Summarize environmental impacts and local environmental controls 4.5.1 Material safety data sheet (MSDS)/documentation for handling and disposal 4.5.1.1 Proper battery disposal 4.5.1.2 Proper toner disposal 4.5.1.3 Proper disposal of other devices and assets 4.5.2 Temperature, humidity-level awareness, and proper ventilation 4.5.2.1 Location/equipment placement 4.5.2.2 Dust cleanup 4.5.2.3 Compressed air/vacuums 4.5.3 Power surges, under-voltage events, and power failures 4.5.3.1 Battery backup 4.5.3.2 Surge suppressor	N/A	Common Safety Procedures – pg. 149 N/A Personal Safety Procedures – pg. 150 N/A Environmental Impacts – pg. 151 N/A Local Environmental Controls – pg. 152 N/A Power Surges and Failures – pg. 153 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 4 Video time - 00:26:54 Exercise Lab time - 00:04:00 Workbook time - 00:35:00	**Content, Licensing, and Policies** Chain of Custody Inform Authorities Hard Drive Integrity Incident Documentation Valid and Non-Expired Licenses Personal Use vs. Corporate Licenses Open-Source Licenses Credit Card Transactions Government Issued and PII Healthcare Data Data Retention Requirements Communication and Professionalism Professional Appearance and Attire Proper Language Positive Attitude and Confidence Listen and Take Notes Cultural Sensitivity Punctuality Avoid Distractions Avoid Arguments Customer Problems and Judgment Clarify Customer Statements Social Media Disclosure Avoidance Offer Repair/Replacement Options Provide Documentation for Services Follow Up with Customer Deal with Confidential Material	4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts 4.6.1 Incident response 4.6.1.1 Chain of custody 4.6.1.2 Inform management/law enforcement as necessary 4.6.1.3 Copy of drive (data integrity and preservation) 4.6.1.4 Documentation of incident 4.6.2 Licensing/digital rights management (DRM)/end-user license agreement (EULA) 4.6.2.1 Valid licenses 4.6.2.2 Non-expired licenses 4.6.2.3 Personal use license vs. corporate use license 4.6.2.4 Open-source license 4.6.3 Regulated data 4.6.3.1 Credit card transactions 4.6.3.2 Personal government-issued information 4.6.3.3 PII 4.6.3.4 Healthcare data 4.6.3.5 Data retention requirements 4.7 Given a scenario, use proper communication techniques and professionalism 4.7.1 Professional appearance and attire 4.7.1.1 Match the required attire of the given environment 4.7.1.1.1 Formal 4.7.1.1.2 Business casual 4.7.2 Use proper language and avoid jargon, acronyms, and slang, when applicable 4.7.3 Maintain a positive attitude/project confidence 4.7.4 Actively listen, take notes, and avoid interrupting the customer 4.7.5 Be culturally sensitive 4.7.5.1 Use appropriate professional titles, when applicable 4.7.6 Be on time (if late, contact the customer) 4.7.7 Avoid distractions 4.7.7.1 Personal calls 4.7.7.2 Texting/social media sites 4.7.7.3 Personal interruptions 4.7.8 Dealing with difficult customers or situations 4.7.8.1 Do not argue with customers or be defensive 4.7.8.2 Avoid dismissing customer problems 4.7.8.3 Avoid being judgmental 4.7.8.4 Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding) 4.7.8.5 Do not disclose experience via social media outlets 4.7.9 Set and meet expectations/timeline and communicate status with the customer 4.7.9.1 Offer repair/replacement options, as needed 4.7.9.2 Provide proper documentation on the services provided 4.7.9.3 Follow up with customer/user at a later date to verify satisfaction 4.7.10 Deal appropriately with customers' confidential and private materials 4.7.10.1 Located on a computer, desktop, printer, etc.	Licensing	Incident Response – pg. 155 N/A Licensing – pg. 156 N/A Regulated Data – pg. 157 N/A Professionalism – pg. 158 N/A Distractions and Difficult Customers – pg. 159 N/A Meeting Customer Expectations – pg. 160 N/A

Lesson	Lesson Topic and Subtopics	Objectives	Exercise Labs	Workbook Projects and Files
Lesson 5 Video time - 00:31:16 Exercise Lab time - 00:32:00 Workbook time - 00:25:00	**Scripting Basics** Batch Files PowerShell Files Visual Basic Script Files Shell Files JavaScript Files Python Files Automation and Restarts Network Drives and Installs Automated Backups Information Gathering Initiating Updates Unintentionally Introducing Malware Inadvertent System Settings Changes Resource Mishandling Remote Access Technologies RDP VPN VNC SSH RMM MSRA Third-Party Tools Security Considerations	4.8 Identify the basics of scripting 4.8.1 Script file types 4.8.1.1 .bat 4.8.1.2 .ps1 4.8.1.3 .vbs 4.8.1.4 .sh 4.8.1.5 .js 4.8.1.6 .py 4.8.2 Use cases for scripting 4.8.2.1 Basic automation 4.8.2.2 Restarting machines 4.8.2.3 Remapping network drives 4.8.2.4 Installation of applications 4.8.2.5 Automated backups 4.8.2.6 Gathering of information/data 4.8.2.7 Initiating updates 4.8.3 Other considerations when using scripts 4.8.3.1 Unintentionally introducing malware 4.8.3.2 Inadvertently changing system settings 4.8.3.3 Browser or system crashes due to mishandling of resources 4.9 Given a scenario, use remote access technologies 4.9.1 Methods/tools 4.9.1.1 RDP 4.9.1.2 VPN 4.9.1.3 Virtual network computer (VNC) 4.9.1.4 Secure Shell (SSH) 4.9.1.5 Remote monitoring and management (RMM) 4.9.1.6 Microsoft Remote Assistance (MSRA) 4.9.1.7 Third-party tools 4.9.1.7.1 Screen-sharing software 4.9.1.7.2 Video-conferencing software 4.9.1.7.3 File transfer software 4.9.1.7.4 Desktop management software 4.9.2 Security considerations of each access method	Automated Tasks Scripting Information Gathering PowerShell Commands Resource Mishandling RDP VPN Connection MRSA	Script File Types – pg. 162 N/A Use Cases for Scripting – pg. 163 N/A Script Usage Considerations – pg. 164 N/A Remote Access Technologies – pg. 165 N/A Third-Party Tools for Remote Access – pg. 166 N/A
Post-Assessment Assessment time - 01:00:00	Operational Procedures: Post-Assessment			