

Professor Messer's  
**CompTIA A+**

**CORE 2** 220-1002  
**Practice Exams**

James "Professor" Messer

# **Professor Messer's**

# **CompTIA 220-11002**

# **A+ Core 2**

# **Practice Exams**

by James “Professor” Messer



<http://www.ProfessorMesser.com>

## **Professor Messer's CompTIA 220-1100 A+ Core 2 Practice Exams**

Written by James "Professor" Messer

Copyright © 2020 by Messer Studios, LLC

<https://www.ProfessorMesser.com>

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher.

First Edition: August 2020

This is version 1.06.

### **Trademark Acknowledgments**

All product names and trademarks are the property of their respective owners, and are in no way associated or affiliated with Messer Studios LLC.

"Professor Messer" is a registered trademark of Messer Studios LLC.

"CompTIA," "A+," "Network+," and "Security+" are registered trademarks of CompTIA, Inc.

### **Warning and Disclaimer**

This book is designed to provide information about the CompTIA 220-1100 Core 2 A+ certification exam. However, there may be typographical and/or content errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. The author shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book.

# Contents

## Introduction

The CompTIA A+ Core 2 Certification .....	i
How to Use This Book .....	ii

## Practice Exam A

Performance-Based Questions .....	1
Multiple Choice Questions .....	5
Multiple Choice Quick Answers .....	33
Detailed Answers .....	35

## Practice Exam B

Performance-Based Questions .....	129
Multiple Choice Questions .....	133
Multiple Choice Quick Answers .....	161
Detailed Answers .....	163

## Practice Exam C

Performance-Based Questions .....	259
Multiple Choice Questions .....	263
Multiple Choice Quick Answers .....	291
Detailed Answers .....	293

## About the Author

James Messer is an information technology veteran whose career has included supercomputer operations, system administration, network management, and IT security.

James is also the founder and CEO of Messer Studios, a leading publisher of training materials for IT certification exams. With over 100 million videos viewed and 435,000 subscribers, Professor Messer's training has helped thousands of students realize their goals of a profession in information technology.

# Introduction

The CompTIA A+ is one of the most popular IT certifications in the industry, and I think it's also one of the most enjoyable study experiences. Whether you're just getting started in information technology or you're a seasoned veteran, you have to appreciate the vast array of hardware and software that's covered in the A+ exams. If you love technology, then the A+ certification is for you.

I've created these sample exams to help you learn what you'll need to pass the exam, but I also hope they provide some additional context and knowledge that you can use once the certification process is over.

In information technology, the learning process never ends. I wish you the best success on your journey!

- Professor Messer

## The CompTIA A+ Core 2 Certification

The 220-1102 A+ Core 2 certification covers many different topics, and includes everything from IT security to software troubleshooting. Here's the breakdown of each domain and the percentage of each topic on the 220-1102 A+ exam:

Domain 1.0 - Operating Systems- 27%

Domain 2.0 - Security - 24%

Domain 3.0 - Software Troubleshooting - 26%

Domain 4.0 - Operational Procedures- 23%

The practice exams in this book follow this breakdown, so you should find that the distribution of questions on a practice exam will be very similar to what you'll see on the actual exam.

# How to Use This Book

This book contains three separate 90-question practice exams; Exam A, Exam B, and Exam C. The exams are designed to emulate the format and complexity of the actual Core 2 A+ exam.

- Take one exam at a time. The difficulty levels are similar between exams, so it doesn't matter which exam you take first.
- The 220-1002 A+ exam is 90 minutes in length, so try setting a timer when you start your practice exam. Time management is an important part of the exam.
- The first section of each practice exam is the list of questions. There's a link next to every question ("Quick Answer" or "The Details") that will jump immediately to the quick answer page or the detailed answer page. If you're using the digital version, your PDF reader keys can quickly jump back to the question page. Adobe Reader in Windows uses **Alt-Left arrow** and macOS Preview uses **Command-[** to move back to the previous view. Be sure to check your PDF reader for specific navigation options.
- The quick answer page is a consolidated list of the answers without any detail or explanation. If you want to quickly check your answer sheet, this is the page for you.
- A detailed answer is available for each exam question. This section repeats the question, the possible answers, and shows the answer with a detailed explanation. This section is formatted to show only one answer per page to avoid giving away the answer to any other questions. Digital readers can use your PDF reader's back button to quickly jump back to the questions.
- As you go through the exam, write down the answers on a separate sheet of paper. You can check the answers after the 90 minutes have elapsed.
- You can grade your results against the quick answer page. For incorrect responses, be sure to check the detailed answer pages for information on why certain answers were considered correct or incorrect.
- After each detailed answer, a video link is available for more information on the topic. You can click the link in your PDF or use your camera to view the QR (Quick Response) code on the page. Your camera app will provide a notification message that will launch the video page in your browser. The URL is also provided for manual entry.

You have the option of using each practice test as a 90 minute timed exam, or as a casual Q&A. Try stepping through each question, picking an answer, and then jumping to the detailed explanation to learn more about each possible answer.

Here's a scoring chart:

**Less than 63 questions correct / 70% and lower** - Use the exam objectives at the end of each detailed answer to determine where you might need some additional help.

**63 to 72 questions correct / 70% to 80%** - You're so close! Keep working on the areas you're missing and fill in those gaps.

**73 to 81 questions correct / 80% to 90%** - This is a strong showing, but some additional studying will help you earn points on the real exam.

Although the actual 220-1002 A+ exam does not calculate the final score as a percentage, getting an 85% on the practice exam can be roughly considered a passing grade.

**More than 81 questions correct / over 90%** - You're ready for the real thing! Book your exam and pass your 220-1002 A+ exam!

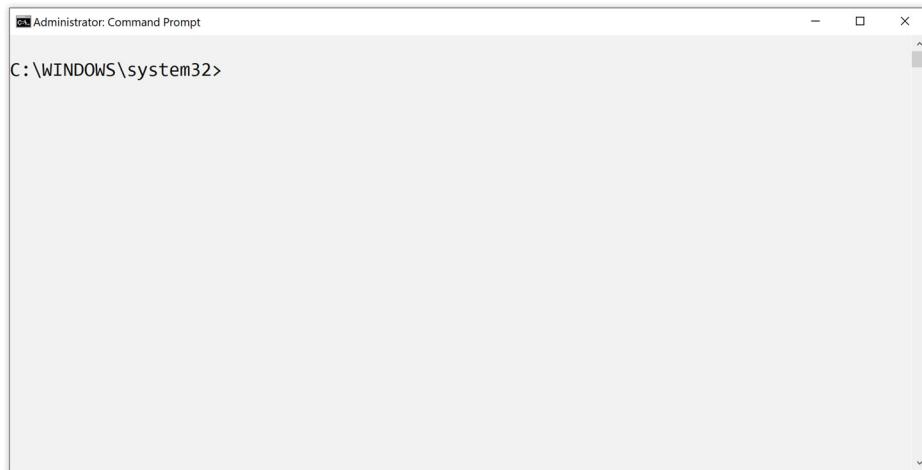
The detailed answer pages break down every correct answer and every incorrect answer. Although it's useful to know when you got a question right, it's more important if you understand exactly why a question was marked wrong. If you understand all of the technologies on these sample exams, then you'll be ready for the real thing.



# Practice Exam A

## Performance-Based Questions

- A1. A technician has recently removed malware from a Windows computer, but the technician is concerned that some of the system files may have been modified. From the command line, analyze and repair any damaged operating system files.



The screenshot shows a Windows Command Prompt window with the title bar 'Administrator: Command Prompt'. The window is minimized. The path 'C:\WINDOWS\system32>' is visible at the top of the command line area.

- A2.** A technician has been tasked with removing malware from a desktop computer. Arrange these malware removal tasks in the correct order to successfully remove the malware.

Schedule scans and run updates
Educate the end user
Enable System Restore
Quarantine infected systems
Remediate
Identify malware symptoms
Disable System Restore

---

- A3.** Match the technology with the description.

Some descriptions will not have a match.

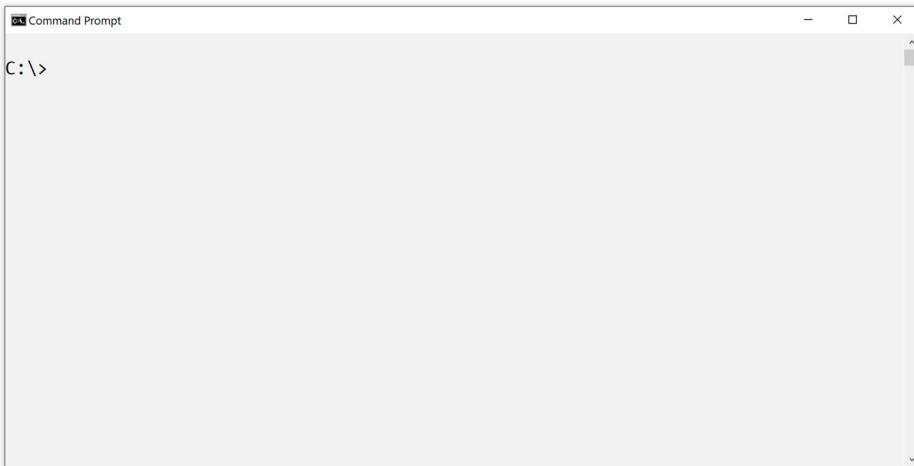
**Technologies:**

EULA
PII
PCI DSS
FOSS

**Descriptions:**

European Union citizens can request to have all personal data removed
Software can be used on one computer and one copy can be stored for backup purposes
A database includes all client first names, last names, and home addresses
All blood test results are stored on laboratory file servers
The software includes source code and can be distributed at no cost
Any credit card numbers stored locally must be encrypted

- A4.** A user needs to access a file located on the \\gate-room server. The file is located in a share called ship-diagnostics. Use the command line to connect to this share using drive g:.



- 
- A5.** Match the commands to the description.  
Some descriptions will not have a match.

**Commands:**

**Descriptions:**

dir	Make changes to a WIM image
taskkill	Repair logical file system errors
diskpart	Change to a different working directory
dism	Terminate a process by PID
	List the contents of a Windows directory
	List the volume names on a storage drive
	Verify group policy settings for a user



# Practice Exam A

## Multiple Choice Questions

A6. A system administrator is installing a new server into the metal racks in a data center. During the installation process, the administrator can feel a faint tingling sensation when mounting the server. Which of the following safety systems should be tested and verified FIRST?

- A. Equipment grounding
- B. Lighted exit signs
- C. Cable management
- D. Waste disposal regulations

Quick  
Answer: 33

The Details: 41

A7. A user has opened a help desk ticket regarding the battery life on their mobile phone. The battery in the phone held a charge for most of the day prior to connecting to the corporate network. The battery now only lasts about half a day and the back of the phone is warmer than usual.

The phone is configured as follows:

Storage: 116.2 GB of 256 GB used

Display and Brightness: Automatic

Wi-Fi: Enabled

Auto-lock: Disabled

VPN: Not connected

Low Power Mode: Disabled

Battery Maximum Capacity: 100%

Which of the following changes would have the BEST impact on battery performance?

- A. Enable auto-lock
- B. Connect to the VPN
- C. Increase available storage space
- D. Disable Wi-Fi

Quick  
Answer: 33

The Details: 42

- A8.** A user in the accounting department has received this error message: "The print spooler service is not running." The user contacts the help desk and opens a ticket for assistance. The help desk technician performs some testing and identifies the issue. Which of these would be the best NEXT step?
- A.** Reinstall all printer drivers
  - B.** Restart the spooler service
  - C.** Reboot the computer
  - D.** Power cycle the printer
- A9.** A student would like to prevent the theft of their laptop while studying at the library. Which of the following security methods would be the BEST choice to protect this laptop?
- A.** Biometrics
  - B.** Locking cabinet
  - C.** USB token
  - D.** Cable lock
- A10.** Rodney, a desktop technician, is cleaning the outside of computers used on a manufacturing assembly line. The assembly line creates sawdust and wood chips, so most of the computers are protected with enclosed computer cases. Which of the following would be the MOST important item for Rodney to include during this cleaning process?
- A.** Surge suppressors
  - B.** Temperature sensors
  - C.** Face masks
  - D.** ESD mats

Quick  
Answer: 33

The Details: 44

Quick  
Answer: 33

The Details: 45

Quick  
Answer: 33

The Details: 46

- A11.** George, a sales manager, has recently replaced a broken mobile phone with a newer version. After receiving the new phone, he restored all of his apps and data from a recent backup. However, when he attempts to download any new email messages he receives a message, “Unable to decrypt email.” Which of the following steps should a technician follow to resolve this issue?
- A. Install the latest operating system patches
  - B. Delete the email app and reinstall
  - C. Restart the phone
  - D. Install the user's private keys
- A12.** The motherboard of a server in the corporate data center has started smoking, and flames can be seen inside the computer case. Which of the following would be the BEST way to extinguish this fire?
- A. An extinguisher with water
  - B. A foam-based extinguisher
  - C. Disconnect the power
  - D. A carbon dioxide extinguisher
- A13.** Which of these Windows features provides full disk encryption for all data on a storage drive?
- A. Domain Services
  - B. EFS
  - C. BranchCache
  - D. BitLocker
- A14.** Which of the following governmental policies manages the use of personal data?
- A. PCI DSS
  - B. EULA
  - C. GDPR
  - D. FOSS

**A15.** A user in the accounting department has recently installed a new app on their Android tablet. The app was not downloaded from the central app store, but instead was downloaded directly from a website as an .apk file. Which of the following would describe this installation process?

- A.** Cloud service
- B.** Sideloaded
- C.** Biometrics
- D.** Encrypted

Quick  
Answer: 33

The Details: 51

**A16.** A help desk technician has been given a network diagram that shows switch interfaces grouped by VLAN. Which of the following would BEST describe this documentation?

- A.** Logical diagram
- B.** Knowledge base
- C.** Inventory management
- D.** Operational procedures

Quick  
Answer: 33

The Details: 52

**A17.** A system administrator is troubleshooting an older application on a Windows 10 computer and needs to modify the UAC process. Which of the following options would provide access to these settings?

- A.** Device Manager
- B.** System Information
- C.** Event Viewer
- D.** User Accounts

Quick  
Answer: 33

The Details: 53

**A18.** An office power system occasionally experiences minor voltage spikes during the business day. Which of the following would be the BEST way to address this power issue?

- A.** Power down when not actively working
- B.** Confirm that the building has an electrical ground
- C.** Connect a surge suppressor to each system
- D.** Maintain an inventory of replacement power supplies

Quick  
Answer: 33

The Details: 54

- A19.** What is the maximum amount of RAM supported by a 32-bit version of an operating system?
- A. 4 GB
  - B. 8 GB
  - C. 16 GB
  - D. 192 GB
- Quick  
Answer: 33  
The Details: 55
- A20.** Daniel, a user, is attempting to start an application on his laptop computer. Each time the application shows the starting graphic, it suddenly disappears and the application icon disappears from the taskbar. A technician would like to get more information about each previous occurrence of the application crash. Which of these choices would provide these details?
- A. Event Viewer
  - B. Task Manager
  - C. Startup Repair
  - D. Safe Mode
- Quick  
Answer: 33  
The Details: 56
- A21.** Which of the following would be unnecessary if a rainbow table is used?
- A. Spoofing
  - B. Social engineering
  - C. Brute force attack
  - D. DDoS
- Quick  
Answer: 33  
The Details: 57
- A22.** A system administrator is upgrading an email service in the corporate data center. During the upgrade, an error message appears and the upgrade fails. Subsequent attempts to perform the upgrade also fail. Which of the following processes should the system administrator follow to return the email server to its previous state?
- A. Backout plan
  - B. Disaster recovery plan
  - C. Incident response plan
  - D. Power plan
- Quick  
Answer: 33  
The Details: 58

**A23.** A user in the shipping department has opened a help desk ticket for problems found when browsing to certain Internet sites. The user also has slow access to other sites and difficulty sending and receiving emails from the local email server. A technician performs some basic troubleshooting and finds that CPU utilization is low, memory usage is minimal, and half of network pings return a response. Which of the following would be the best NEXT troubleshooting step?

- A.** Remove all startup applications and reboot the computer
- B.** Restart in Safe Mode and repeat the tests
- C.** Check the statistics on the user's switch port
- D.** Scan with an anti-malware utility

Quick  
Answer: 33

The Details: 59

**A24.** A system administrator has created a shared folder on a server to store operating system images. Technicians will access the shared folder to download the latest images when performing large-scale system installations. Which of the following will be the MOST likely method of accessing this data?

- A.** Map the shared folder to an available drive letter
- B.** Download the shared folder through a proxy
- C.** Link the images to a cloud storage service
- D.** Access the folder using a remote access client

Quick  
Answer: 33

The Details: 60

**A25.** A desktop administrator is installing a 64-bit version of Windows 10 Pro on a workstation, but the installation will not start. The workstation configuration is:

- 1 GHz CPU
- 2 GB of RAM
- 15 GB of free storage space
- 1280 x 720 video resolution

Which of the following would allow this installation to proceed?

- A.** Increase free storage space to 20 GB Quick  
Answer: 33
- B.** Decrease resolution to 800 x 600
- C.** Upgrade to a faster processor The Details: 61
- D.** Increase RAM to 4 GB

**A26.** A security technician has identified malware that is running as part of the OS kernel. Traditional anti-malware scans were not able to identify any problems on the computer. Which of the following would be the BEST description of this malware?

- A.** Rootkit Quick  
Answer: 33
- B.** Worm
- C.** Botnet The Details: 62
- D.** Crypto-malware

**A27.** A help desk technician has been called to a training room that uses Android tablets as presentation devices. An application used for the training program will not start on any of the tablets. When the application is selected, the splash screen appears for a moment and then completely disappears with no error message. Which of the following would be the best NEXT troubleshooting step?

- A.** Install all operating system updates Quick  
Answer: 33
- B.** Uninstall the application
- C.** Power cycle the tablets The Details: 63
- D.** Roll back to the previous application version

- A28.** A user on the headquarters network has opened a help desk ticket about their Windows desktop. When starting their computer, the login process proceeds normally but the Windows desktop takes fifteen minutes to appear. Yesterday, the desktop would appear in just a few seconds. Which of the following would be the MOST likely reason for this issue?
- A.** Slow profile load
  - B.** Incorrect boot device order
  - C.** Faulty RAM
  - D.** Incorrect username and password
- A29.** A system administrator has been asked to install a new application on a server, but the application is 64-bit and the server operating system is 32-bit. Which of the following describes the issue associated with this installation?
- A.** File permissions
  - B.** OS compatibility
  - C.** Installation method
  - D.** Available drive space
- A30.** A security guard has reported that a person was seen passing through a secure door without using a door badge. The intruder slipped through the door by closely following the person in front of them. Which of these would best describe these actions?
- A.** Dumpster diving
  - B.** Brute force
  - C.** Phishing
  - D.** Tailgating

Quick  
Answer: 33

The Details: 64

Quick  
Answer: 33

The Details: 65

Quick  
Answer: 33

The Details: 66

**A31.** A Linux administrator needs to create a system image of a laptop used by the help desk for network troubleshooting. Which of the following utilities would provide this functionality?

- A.** dd
- B.** sudo
- C.** ifconfig
- D.** apt-get

Quick  
Answer: 33

The Details: 67

**A32.** An internal audit has found that a server in the DMZ has been participating in DDoS attacks against external devices. What type of malware would be MOST likely found on this server?

- A.** Worm
- B.** Rootkit
- C.** Keylogger
- D.** Spyware
- E.** Botnet

Quick  
Answer: 33

The Details: 68

**A33.** A user has delivered a broken laptop to the help desk, and he's visibly upset and quite vocal about the problem he's having. He's also asking for a very specific repair that doesn't appear to have any relationship to his issue. What's the best way to handle this situation?

- A.** Repeat your understanding of the issue to the customer and provide an estimate and follow-up time
- B.** Refuse the repair until the customer calms down
- C.** Inform the customer of his mistake with the proposed repair
- D.** Refuse to make any commitments until the computer is examined

Quick  
Answer: 33

The Details: 69

- A34.** Daniel, a user in the finance department, has purchased a new Android smartphone and has installed a number of productivity apps. After a day of use, Daniel finds that the battery is draining rapidly, even when the phone is not being used. Which of the following tasks should Daniel perform after completing a factory reset?
- A. Disable Bluetooth
  - B. Check app sharing permissions
  - C. Run a speed test on the cellular connection
  - D. Scan each app before installation
- A35.** A network administrator has configured all of their wireless access points with WPA2 security. Which of the following technologies would be associated with this configuration?
- A. RC4
  - B. TACACS
  - C. TKIP
  - D. AES
- A36.** A user has reported that all Google search results in their Internet browser are displaying a non-Google website. This redirection occurs each time a Google search is attempted. Which of the following would be the BEST way to prevent this issue in the future?
- A. Windows Firewall
  - B. MAC filtering
  - C. Port security
  - D. Certificate-based authentication
  - E. Anti-malware utility

**A37.** A user has installed multiple applications over the last week. During the startup process, the computer now takes over fifteen minutes to display the Windows desktop. Which of the following utilities would help the system administrator troubleshoot this issue?

- A.** defrag
- B.** dism
- C.** msconfig
- D.** robocopy

Quick  
Answer: 33

The Details: 73

**A38.** A server administrator is replacing the memory in a database server. Which of the following steps should be followed FIRST?

- A.** Remove the existing memory modules
- B.** Wear an air filter mask
- C.** Disconnect all power sources
- D.** Connect an ESD strap

Quick  
Answer: 33

The Details: 74

**A39.** A technician is dismantling a test lab for a recently completed project, and the lab manager would like to use the existing computers on a new project. However, the security administrator would like to ensure that none of the data from the previous project is accessible on the existing hard drives. Which of the following would be the best way to accomplish this?

- A.** Quick format
- B.** Degauss the drives
- C.** Regular format
- D.** Reinstall the operating system

Quick  
Answer: 33

The Details: 75

**A40.** A system administrator needs to view a set of application log files contained in a folder named “logs.” Which of the following commands should be used to make this the current active directory?

- A.** cd logs
- B.** mv logs
- C.** dir logs
- D.** md logs

Quick  
Answer: 33

The Details: 76

- A41.** Which of the following technologies would be the best choice to boot computers in a training room over the network?
- A. MBR
  - B. NTFS
  - C. Dual boot
  - D. PXE
- A42.** Which of these OS installation types uses an XML file that answers all of the questions normally provided during the installation?
- A. Unattended
  - B. Image
  - C. PXE
  - D. Clean
- A43.** A user has noticed that their system has been running very slowly over the last few days. They have also noticed files stored on their computer randomly disappear after the files are saved. The user has rebooted the computer, but the same problems continue to occur. Which of the following should the user perform to resolve these issues?
- A. Boot to Safe Mode
  - B. Release and renew the network connection
  - C. Install anti-malware software
  - D. Upgrade the system RAM
- A44.** A user in the sales department has opened a help desk ticket to report a dim display on their tablet. When they use the tablet in the office, the screen brightness is normal. In meetings with customers, the display appears much dimmer. Which of these would be the MOST likely reason for this difference?
- A. The tablet display is faulty
  - B. The tablet is brighter when connected to power
  - C. The tablet backlight is on a timer
  - D. Indoor LED lighting is causing the display to dim

Quick  
Answer: 33

The Details: 77

Quick  
Answer: 33

The Details: 78

Quick  
Answer: 33

The Details: 79

Quick  
Answer: 33

The Details: 80

- A45.** The hard drive in a macOS desktop has failed and none of the data on the drive was recoverable. A new storage drive has now been installed. Which of the following should be used to restore the data on the computer?
- A. Backup and Restore
  - B. Boot Camp
  - C. Time Machine
  - D. Disk Utility
- A46.** A user purchased a copy of home tax software and has installed it on their company computer. This morning, the user logs in and finds that the tax software has been automatically removed from the system. Which of the following would be the MOST likely reason for this result?
- A. The company per-seat licenses are all in use
  - B. The software uses a FOSS license
  - C. The user has installed a personal license
  - D. The software is subject to the GDPR
- A47.** A system administrator is upgrading four workstations from Windows 8.1 to Windows 10. All of the user files and applications are stored on the server, and no documents or settings need to be retained between versions. Which of these installation methods would be the BEST way to provide this upgrade?
- A. Factory reset
  - B. Repair installation
  - C. Clean install
  - D. Multiboot
- A48.** A computer on a manufacturing floor has been identified as a malware-infected system. Which of the following should be the best NEXT step to resolve this issue?
- A. Disconnect the network cable
  - B. Perform a malware scan
  - C. Disable System Restore
  - D. Download the latest anti-malware signatures

Quick  
Answer: 33

The Details: 81

Quick  
Answer: 33

The Details: 82

Quick  
Answer: 33

The Details: 83

Quick  
Answer: 33

The Details: 84

- A49.** A technician has been called to resolve an issue with a networked laser printer that is not printing. When the technician arrives on-site, they find the printer will require a hardware replacement. All hardware is managed by a third-party and will take a week before the printer is operational again. Which of the following would be the technician's best NEXT step?
- A.** Work on the next ticket in the queue
  - B.** Add a follow-up event for one week later
  - C.** Inform the user of the repair status
  - D.** Order a printer maintenance kit
- A50.** An administrator is upgrading a Windows 8.1 Enterprise x64 computer to Windows 10. The user would like to maintain all applications and files during the upgrade process. Which of the following upgrade options would meet this requirement?
- A.** Windows 10 Enterprise x86
  - B.** Windows 10 Pro x64
  - C.** Windows 10 Enterprise x64
  - D.** Windows 10 Pro x86
- A51.** A user in the marketing department is using an application that randomly shuts down during normal use. When the problem occurs, the application suddenly disappears and no error messages are shown on the screen. Which of the following would provide the system administrator with additional information regarding this issue?
- A.** System Configuration
  - B.** Event Viewer
  - C.** Device Manager
  - D.** Local Security Policy
  - E.** SFC

Quick  
Answer: 33

The Details: 85

Quick  
Answer: 33

The Details: 86

Quick  
Answer: 33

The Details: 87

**A52.** A workstation on a manufacturing floor is taking much longer than normal to boot. Which of the following would be the BEST way to troubleshoot this issue?

- A.** Replace the CPU
- B.** Disable the startup applications
- C.** Upgrade the RAM
- D.** Install the latest OS patches

Quick  
Answer: 33

The Details: 88

**A53.** A Windows 10 user is installing a new application that also installs a service. Which of the following permissions will be required for this installation?

- A.** Guest
- B.** Power User
- C.** Administrator
- D.** Standard user

Quick  
Answer: 33

The Details: 89

**A54.** A user working from home is not able to print to a laser printer at the corporate office. Which of the following would be the MOST likely reason for this issue?

- A.** DLP policy
- B.** Outdated anti-virus signatures
- C.** Disconnected VPN
- D.** MDM configuration

Quick  
Answer: 33

The Details: 90

**A55.** An employee has modified the NTFS permissions on a local file share to provide read access to Everyone. However, users connecting from a different computer do not have access to the file. Which of the following is the reason for this issue?

- A.** The NTFS permissions were not synchronized
- B.** Share permissions restrict access from remote devices
- C.** The user is an Administrator
- D.** Remote users are connecting with Guest accounts

Quick  
Answer: 33

The Details: 91

**A56.** A healthcare company has replaced some of their desktop computers with laptops and will be disposing of the older computers. The security administrator would like to guarantee that none of the existing data on the hard drives could be recovered once the systems are sent to the recycling center. Which of the following methods would meet this requirement?

- A.** Quick format
- B.** Reinstall the OS
- C.** Remove all user folders
- D.** Shred the drives

Quick  
Answer: 33

The Details: 92

**A57.** A technician has been assigned a support ticket that urgently requests a laptop repair, but there are already many open support tickets ahead of this request. The technician doesn't recognize the name associated with the ticket. Which of these choices would be the best path to take?

- A.** Place the ticket into the queue as first-come, first-served
- B.** Prioritize the support tickets by device type
- C.** Triage the queue and prioritize the tickets in order of repair complexity
- D.** Contact the end-user and determine the urgency of the repair

Quick  
Answer: 33

The Details: 93

**A58.** A user has received a pop up message on their computer that states applications on their computer are infected with a virus. A technician has determined that the pop up message is a hoax that needs to be removed from the computer. The technician has disabled System Restore to remove all previous restore points. Which of the following tasks would be the best NEXT step?

- A.** Update the anti-virus signatures
- B.** Educate the end-user
- C.** Schedule anti-virus scans for midnight each day
- D.** Boot the system with a pre-installation environment

Quick  
Answer: 33

The Details: 94

**A59.** A network administrator needs to manage a switch and firewall at a remote location. Which of the following would be the BEST choice for this requirement?

- A.** RDP
- B.** Telnet
- C.** SSH
- D.** VNC

Quick  
Answer: 33

The Details: 95

**A60.** A user has placed a smartphone on their desk, and they occasionally hear the sound of a camera shutter when the phone is not being used. Which of the following should a technician follow to BEST resolve this issue?

- A.** Put the phone into airplane mode
- B.** Connect to the corporate network using a VPN connection
- C.** Run an anti-malware scan on the smartphone
- D.** Remove any paired Bluetooth devices

Quick  
Answer: 33

The Details: 96

**A61.** Sam, a user on the research and development team, reports that her computer displays the message “Missing operating system” during boot. A technician runs hardware diagnostics and finds that the RAM, CPU, storage drive, and power supply all pass the tests. The technician then finds that a connected USB flash drive was causing the issue. Which of the following would prevent this issue from occurring in the future?

- A.** Update the BCD
- B.** Install the latest OS patches
- C.** Run SFC
- D.** Modify the BIOS boot order

Quick  
Answer: 33

The Details: 97

- A62.** Jack, a user, has opened a help desk ticket relating to email messages he's receiving. The messages appear to be replies to a message that Jack did not send. Most of the messages contain information about third-party product promotions and sales information. Which of the following is the MOST likely cause of these messages?
- A. Man-in-the-middle
  - B. Corrupted email database
  - C. Adware
  - D. Hijacked email
- Quick  
Answer: 33  
The Details: 98
- A63.** In which of the following file types would a system administrator expect to see the command, "cd c:\source"?
- A. .sh
  - B. .vbs
  - C. .py
  - D. .bat
- Quick  
Answer: 33  
The Details: 99
- A64.** A malware infection has recently been removed from a computer. When starting the operating system, Windows shows errors during the startup process indicating some core operating system files are missing. Which of the following should be used to restore these missing files?
- A. gpupdate
  - B. dism
  - C. sfc
  - D. diskpart
- Quick  
Answer: 33  
The Details: 100

**A65.** A desktop administrator has determined that an employee in the corporate office has been using their computer to share copyrighted materials to others on the Internet. Which of the following should be the best NEXT step?

- A.** Create a firewall rule to block Internet access to this computer
- B.** Create a hash for each file that was shared
- C.** Compile a list of licenses for each set of copyrighted materials
- D.** Retrieve and securely store the computer

Quick  
Answer: 33

The Details: 101

**A66.** A system administrator would like to require a specific password complexity for all Active Directory users. Which of the following would be the BEST way to complete this requirement?

- A.** Login script
- B.** Folder redirection
- C.** Port security
- D.** Group Policy

Quick  
Answer: 33

The Details: 102

**A67.** A system administrator is creating a series of shared folders that should not be visible when users browse the network for available shared resources. What symbol should be added to the end of a share name to provide this functionality?

- A.** . (period)
- B.** \$ (dollar sign)
- C.** ! (exclamation mark / bang)
- D.** # (hash sign / number sign)

Quick  
Answer: 33

The Details: 103

- A68.** Jack, a user, is having problems with the 802.11 wireless connection on his iOS phone. Although there are names appearing in the network list, his phone does not show any connectivity to a wireless network. Jack has confirmed that airplane mode is not enabled, Bluetooth is on, and VPN is not enabled. Which of the following is the MOST likely reason for this lack of wireless connectivity?
- A. The phone does not include a data plan
  - B. The wireless network is not active
  - C. The Bluetooth connection is conflicting with the Wi-Fi
  - D. The Wi-Fi password is incorrect
  - E. The wireless radio is disabled
- A69.** A desktop administrator is upgrading the video adapter in a CAD/CAM workstation. Which of the following should the administrator use during this process?
- A. Tone generator
  - B. Anti-static strap
  - C. Safety goggles
  - D. Toner vacuum
- A70.** A help desk director would like to identify and track computer systems that have been returned for service or moved from one location to another. Which of the following would be the BEST solution for these requirements?
- A. Cable labels
  - B. Asset tags
  - C. Topology diagrams
  - D. Login names

- A71.** A technician is troubleshooting a computer infected with a virus. The user thought they were opening a spreadsheet, but the file was actually a virus executable. Which of the following Windows options were MOST likely associated with this issue?
- A. Always show icons, never thumbnails
  - B. Display the full path in the title bar
  - C. Always show menus
  - D. Hide extensions for known file types
- Quick  
Answer: 33  
The Details: 107
- A72.** A financial management company would like to ensure that mobile users are configured with the highest level of wireless encryption while working in the office. They would also like to include an additional user verification step during the login process. Which of the following would provide this functionality? (Choose TWO)
- A. RADIUS
  - B. WPS
  - C. Multi-factor authentication
  - D. TKIP
  - E. TACACS
  - F. RC4
  - G. WPA2
- Quick  
Answer: 33  
The Details: 108
- A73.** A network consulting firm is creating a proposal to upgrade the Internet firewalls for a large corporation. The proposal includes a description of the project and the network topology changes that would be required to support the upgrade. The proposal also describes the risks involved in the process of making this upgrade. Which of the following should be covered NEXT in the proposal?
- A. End-user approvals
  - B. Backout plan
  - C. Change control application
  - D. Detailed upgrade plan
- Quick  
Answer: 33  
The Details: 110

**A74.** An organization has been tasked with increasing the minimum password length. A systems administrator has created a policy to require all passwords to be at least ten characters long for all users. When testing this policy in the lab, a laptop computer allowed the creation of eight-character passwords. Which of the following commands should be used to apply this new policy on the laptop?

- A.** net use
- B.** gpupdate
- C.** sfc
- D.** tasklist

Quick  
Answer: 33

The Details: 111

**A75.** A technician has been tasked with removing malware on a training room laptop. After updating the anti-virus software and removing the malware, the technician creates a backup of the system. After the training class ends, the technician is notified that the malware has returned. Which of the following steps was missed and caused the system to be infected again?

- A.** Boot to a pre-installation environment
- B.** Identify malware symptoms
- C.** Disable System Restore before removal
- D.** Update to the latest BIOS version

Quick  
Answer: 33

The Details: 112

**A76.** A data center manager requires each server to maintain at least fifteen minutes of uptime during a power failure. Which of these would be the BEST choice for this requirement?

- A.** Cloud-based storage
- B.** UPS
- C.** Redundant power supplies
- D.** Surge suppressor

Quick  
Answer: 33

The Details: 113

**A77.** A financial corporation is deploying tablets to their salespeople in the field. The company would like to ensure that the data on the tablets would remain private if the devices were ever stolen or lost. Which of the following would be the BEST way to meet this requirement?

- A.** Use full device encryption
- B.** Require multi-factor authentication
- C.** Install a locator application
- D.** Use a firewall app

Quick  
Answer: 33

The Details: 114

**A78.** A system administrator is adding an additional drive to a server and extending the size of an existing volume. Which of the following utilities would provide a graphical summary of the existing storage configuration?

- A.** Disk Management
- B.** Performance Monitor
- C.** Event Viewer
- D.** Task Scheduler
- E.** Device Manager

Quick  
Answer: 33

The Details: 115

**A79.** While using a laptop during presentations, a company vice president has found that her system randomly locks up. While the problem is occurring, the screen continues to display the last presentation slide but none of the mouse or keyboard buttons will work. To regain control, the vice president must power down and reboot her computer. Which of the following would be the BEST option for troubleshooting this issue?

- A.** Examine the Task Manager
- B.** Install an anti-malware utility
- C.** Run the presentation software in Safe Mode
- D.** Check the Event Viewer

Quick  
Answer: 33

The Details: 116

- A80.** A system administrator has booted a computer using PXE. Which of the following would be the MOST likely reason for this task?
- A. Monthly OS patch install
  - B. OS installation from a network drive
  - C. Boot to Safe Mode
  - D. Control the computer remotely
- Quick Answer: 33  
The Details: 117
- A81.** A user has opened a help desk ticket for application slowdowns and unwanted pop-up windows. A technician updates the anti-virus software, scans, and removes the malware. The technician then schedules future scans and creates a new restore point. Which of the following should be the NEXT step in the removal process?
- A. Disable System Restore
  - B. Update the anti-virus signatures
  - C. Quarantine the system
  - D. Educate the end user
- Quick Answer: 33  
The Details: 118
- A82.** A technician is setting up some new computers on an industrial manufacturing floor that cuts wood boards for cabinets. Which of the following would be the MOST important for this setup process?
- A. ESD mat
  - B. UPS
  - C. Anti-static bag
  - D. Air filter mask
- Quick Answer: 33  
The Details: 119

**A83.** Sam, a user in the accounting department, has opened a help desk ticket due to problems accessing the website of the company's payroll service provider. The help desk technician finds that other users in the accounting department are able to successfully access the website. While testing other website connections on Sam's computer, the technician finds that many pop-up windows are displayed. Which of the following would be the BEST way for the technician to resolve this issue?

- A.** Uninstall the browser and reinstall with a different version
- B.** Restore the workstation from a known good backup
- C.** Start in Safe Mode and connect to the payroll website
- D.** Modify the browser's proxy settings

Quick  
Answer: 33

The Details: 120

**A84.** A business partner in a different country needs to access an internal company server during the very early morning hours. The internal firewall will limit the partner's access to this single server. Which of these would be the MOST important security task to perform on this server?

- A.** Install the latest OS patches
- B.** Remove the server from the Active Directory domain
- C.** Use only 64-bit applications
- D.** Run a weekly anti-virus scan

Quick  
Answer: 33

The Details: 121

**A85.** A Linux administrator has been asked to upgrade the web server software on a device. Which of the following would provide the administrator with the appropriate rights and permissions for this upgrade?

- A.** chmod
- B.** apt-get
- C.** ifconfig
- D.** sudo

Quick  
Answer: 33

The Details: 122

**A86.** A system administrator has installed a new video driver on a laptop computer, but the icons and text on the screen are larger than the previous driver version. Which of the following should be modified to resolve this problem?

- A.** Resolution
- B.** Color depth
- C.** Refresh rate
- D.** Video memory

Quick  
Answer: 33

The Details: 123

**A87.** A network administrator is configuring a wireless network at a small office. The administrator would like to allow wireless access for all computers but exclude a single kiosk in the lobby. Which of the following configuration settings would meet this requirement?

- A.** SSID suppression
- B.** Content filtering
- C.** Static IP addressing
- D.** WPS
- E.** MAC filtering

Quick  
Answer: 33

The Details: 124

**A88.** After booting, a laptop computer is showing a black screen instead of the normal Windows login prompt. The logs from the update server show drivers on the laptop were automatically updated overnight. Which of the following would be the BEST way to resolve this issue?

- A.** Reinstall the operating system
- B.** Update the BCD
- C.** Start in VGA mode and roll back the driver
- D.** Upgrade the BIOS

Quick  
Answer: 33

The Details: 126

**A89.** A security administrator has received an alert that a user's workstation in the shipping department has attempted to communicate to a command and control server for a well-known botnet. The logs on the workstation show that the user manually installed a new Internet browser the previous day. Which of the following would be the BEST next step for troubleshooting this issue?

- A.** Uninstall the new browser
- B.** Backup the user's documents
- C.** Roll back to a previous restore point
- D.** Disable the user's account

Quick  
Answer: 33

The Details: 127

**A90.** A technician is installing a new wireless network in a small remote office. Which of the following should the technician choose to provide the highest level of security on the network?

- A.** WPA2
- B.** MAC filtering
- C.** Static IP addressing
- D.** SSID suppression

Quick  
Answer: 33

The Details: 128



# **Practice Exam A**

## **Multiple Choice Quick Answers**

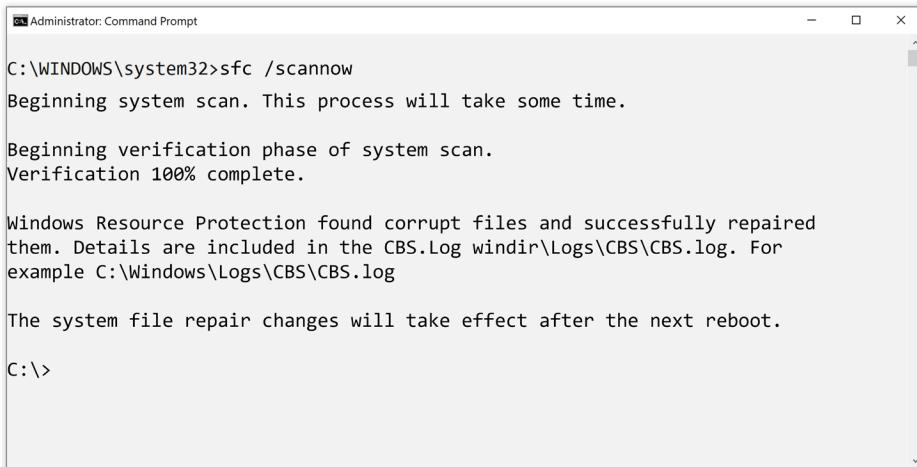
- |        |        |              |
|--------|--------|--------------|
| A6. A  | A36. E | A66. D       |
| A7. A  | A37. C | A67. B       |
| A8. B  | A38. C | A68. D       |
| A9. D  | A39. C | A69. B       |
| A10. C | A40. A | A70. B       |
| A11. D | A41. D | A71. D       |
| A12. D | A42. A | A72. C and G |
| A13. D | A43. C | A73. D       |
| A14. C | A44. B | A74. B       |
| A15. B | A45. C | A75. C       |
| A16. A | A46. C | A76. B       |
| A17. D | A47. C | A77. A       |
| A18. C | A48. A | A78. A       |
| A19. A | A49. C | A79. D       |
| A20. A | A50. C | A80. B       |
| A21. C | A51. B | A81. D       |
| A22. A | A52. B | A82. D       |
| A23. C | A53. C | A83. B       |
| A24. A | A54. C | A84. A       |
| A25. A | A55. B | A85. D       |
| A26. A | A56. D | A86. A       |
| A27. C | A57. D | A87. E       |
| A28. A | A58. A | A88. C       |
| A29. B | A59. C | A89. D       |
| A30. D | A60. C | A90. A       |
| A31. A | A61. D |              |
| A32. E | A62. D |              |
| A33. A | A63. D |              |
| A34. D | A64. C |              |
| A35. D | A65. D |              |



# Practice Exam A

## Detailed Answers

- A1. A technician has recently removed malware from a Windows computer, but the technician is concerned that some of the system files may have been modified. From the command line, analyze and repair any damaged operating system files.



```
Administrator: Command Prompt
C:\WINDOWS\system32>sfc /scannow
Beginning system scan. This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection found corrupt files and successfully repaired them. Details are included in the CBS.Log windir\Logs\CMS\CBS.log. For example C:\Windows\Logs\CMS\CBS.log

The system file repair changes will take effect after the next reboot.

C:\>
```

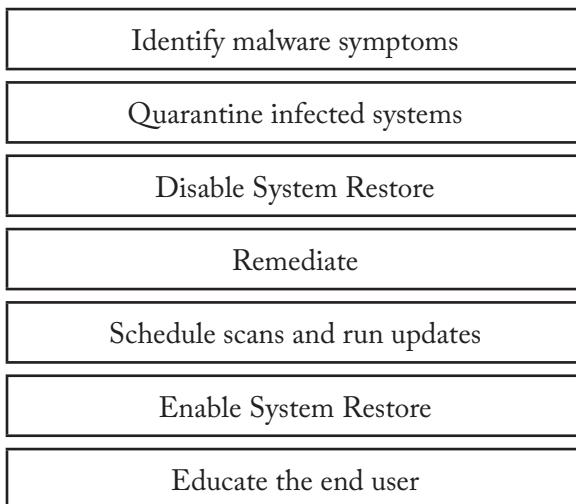
The sfc (System File Checker) utility will scan the integrity of all protected system files and replace any files that may be corrupted.



### More information:

220-1002, Objective 1.4 - Microsoft Command Line Tools  
<https://professormesser.link/1002010401>

- A2.** A technician has been tasked with removing malware from a desktop computer. Arrange these malware removal tasks in the correct order to successfully remove the malware.



To properly remove malware, it's important to follow a strict set of guidelines. Missing one of these steps or following them out of order could cause the malware to remain on the computer or to have it easily reinfect after rebooting.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**A3.** Match the technology with the description.

Some descriptions will not have a match.

**Technologies:**

EULA

**Descriptions:**

Software can be used on one computer and one copy can be stored for backup purposes

The EULA (End User Licensing Agreement) determines how the software can be used by the end user. The user will commonly be required to agree to the terms of the EULA before the software can be installed.

PII

A database includes all client first names, last names, and home addresses

PII (Personally Identifiable Information) is any data that could be associated with an individual. For example, your name, address, phone number, and email address are considered PII.

PCI DSS

Any credit card numbers stored locally must be encrypted

PCI DSS (Payment Card Industry Data Security Standard) is a set of objectives created by the credit card industry to ensure that financial transaction data is stored and transmitted securely.

FOSS

The software includes source code and can be distributed at no cost

FOSS (Free and Open Source) software is distributed for free and usually includes access to the source code of the application.

GDPR

European Union citizens can request to have all personal data removed

The GDPR (General Data Protection Regulation) is a regulation that controls data protection and privacy for individuals in the EU.

PHI

All blood test results are stored on laboratory file servers

PHI (Protected Health Information) is any healthcare data that can be associated with an individual.



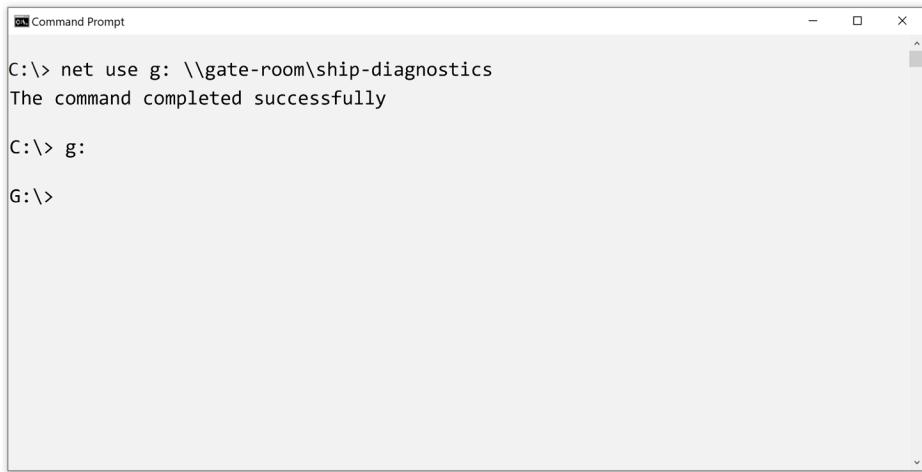
**More information:**

220-1002, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1002040601>

---

- A4.** A user needs to access a file located on the \\gate-room server. The file is located in a share called ship-diagnostics. Use the command line to connect to this share using drive g:.



```
Command Prompt

C:\> net use g: \\gate-room\ship-diagnostics
The command completed successfully

C:\> g:

G:\>
```

The Windows `net use` command is used to map a network share to a drive letter. The syntax is:

`net use drive: \\<servername>\<sharename>`



**More information:**

220-1002, Objective 1.4 - Network Command Line Tools

<https://professormesser.link/1002010402>

**A5.** Match the commands to the description.

Some descriptions will not have a match.

**Commands:**

dir

**Descriptions:**

List the contents of a Windows directory

The dir (directory list) command provides a list of files and directories.

taskkill

Terminate a process by PID

The Windows taskkill command will terminate tasks by process id (PID) or by the name of the executable.

diskpart

List the volume names on a storage drive

Diskpart (Disk Partitioning) provides command line access to disk and partition configuration settings.

dism

Make changes to a WIM image

The dism (Deployment Image Servicing and Management tool) utility is used to managed Windows Imaging Format (WIM) files.

chkdsk

Repair logical file system errors

The chkdsk (Check Disk) command can fix logical file system error and locate and recover data from bad sectors on a hard drive.

cd

Change to a different working directory

The cd (Change Directory) command is used with the backslash (\) to change the working directory to a different volume or folder name.

gpresult

Verify group policy settings for a user

The gpresult (Group Policy Results) utility allows the domain administrator to verify policy settings for a computer or user.



**More information:**

220-1002, Objective 1.4 - Microsoft Command Line Tools

<https://professormesser.link/1002010401>

**A6.** A system administrator is installing a new server into the metal racks in a data center. During the installation process, the administrator can feel a faint tingling sensation when mounting the server. Which of the following safety systems should be tested and verified FIRST?

- A.** Equipment grounding
  - B.** Lighted exit signs
  - C.** Cable management
  - D.** Waste disposal regulations
- 

**The Answer:** **A.** Equipment grounding

Electrical safety is one of the highest priorities because of its association with personal safety. Before a single computer can be turned on, the facility has to be properly grounded and the power systems must be installed properly.

**The incorrect answers:**

**B.** Lighted exit signs

Most building codes will require lighted exit signs, but it's more important to test the electrical system so that nobody is injured during equipment installation.

**C.** Cable management

Proper cable management will help prevent any trip hazards. Before addressing the cable management system, it will be more important to resolve any electrical problems in the facility.

**D.** Waste disposal systems

The waste disposal system would not be a cause of the electrical issues described this in question.



**More information:**

220-1002, Objective 4.4 - Safety Procedures

<https://professormesser.link/1002040401>

- A7.** A user has opened a help desk ticket regarding the battery life on their mobile phone. The battery in the phone held a charge for most of the day prior to connecting to the corporate network. The battery now only lasts about half a day and the back of the phone is warmer than usual.

The phone is configured as follows:

Storage: 116.2 GB of 256 GB used  
Display and Brightness: Automatic  
Wi-Fi: Enabled  
Auto-lock: Disabled  
VPN: Not connected  
Low Power Mode: Disabled  
Battery Maximum Capacity: 100%

Which of the following changes would have the BEST impact on battery performance?

- A.** Enable auto-lock
  - B.** Connect to the VPN
  - C.** Increase available storage space
  - D.** Disable Wi-Fi
- 

**The Answer:** **A.** Enable auto-lock

The backlight of a mobile phone requires constant battery use, and the phone in an active state will use more battery than one that is locked or in a standby state.

**The incorrect answers:**

**B.** Connect to the VPN

Connecting to a VPN would most likely increase the amount of battery used due to the encryption and decryption that would need to occur.

**C. Increase available storage space**

The battery life on a phone is not based on the amount of storage space in use. Increasing storage space would not extend the life of the battery.

**D. Disable Wi-Fi**

Wi-Fi does not have a significant impact on battery performance when compared to the screen backlight and active phone services.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**A8.** A user in the accounting department has received this error message: "The print spooler service is not running." The user contacts the help desk and opens a ticket for assistance. The help desk technician performs some testing and identifies the issue. Which of these would be the best NEXT step?

- A.** Reinstall all printer drivers
  - B.** Restart the spooler service
  - C.** Reboot the computer
  - D.** Power cycle the printer
- 

**The Answer:** **B.** Restart the spooler service

The spooler operates as a background service in Windows. Once the problem is identified and corrected, the spooler service would need to be restarted.

**The incorrect answers:**

**A.** Reinstall all printer drivers

The print spooler service is not dependent on the print drivers.

Reinstalling print drivers would not commonly resolve a problem with the print spooler not running.

**C.** Reboot the computer

Although rebooting the computer may cause the services to restart, it's an unnecessary step that takes time away from problem resolution. It's much easier and faster to simply restart the service.

**D.** Power cycle the printer

If the print spooler service isn't running, then the printer won't receive a print job. Power cycling the printer won't cause the print spooler to restart.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Solutions

<https://professormesser.link/1002030102>

**A9.** A student would like to prevent the theft of their laptop while studying at the library. Which of the following security methods would be the BEST choice to protect this laptop?

- A.** Biometrics
  - B.** Locking cabinet
  - C.** USB token
  - D.** Cable lock
- 

**The Answer:** **D.** Cable lock

A cable lock is portable, it can be installed and uninstalled quickly, and it can be wrapped around an existing table or chair to prevent a computer from theft.

**The incorrect answers:**

**A.** Biometrics

Biometrics, such as fingerprints or face scanning, is useful for preventing access through a door or to an operating system. However, biometrics won't stop someone from physically taking a laptop from a table.

**B.** Locking cabinet

A locking cabinet would certainly prevent a laptop from theft, but it's not a practical security device to carry to a library.

**C.** USB token

A USB token is often used to control the use of certain applications. A USB token will not protect a laptop from being stolen.



**More information:**

220-1002, Objective 2.1 - Physical Security

<https://professormesser.link/1002020101>

**A10.** Rodney, a desktop technician, is cleaning the outside of computers used on a manufacturing assembly line. The assembly line creates sawdust and wood chips, so most of the computers are protected with enclosed computer cases. Which of the following would be the MOST important item for Rodney to include during this cleaning process?

- A. Surge suppressors
  - B. Temperature sensors
  - C. Face masks
  - D. ESD mats
- 

**The Answer:** C. Face masks

A technician working in an area of dust or debris in the air should use a face mask to prevent any particles in the air from entering their lungs.

**The incorrect answers:**

**A.** Surge suppressors

Surge suppressors would protect systems from power surges, but it wouldn't help with the cleaning process on an assembly line.

**B.** Temperature sensors

There's no mention in this question of any temperature issues, so monitoring the temperature during the cleaning process would not be the most important item to include.

**D.** ESD mats

If the technicians were working inside of a computer, then an ESD mat may be important to include. However, this question only mentioned cleaning the outside of the computers.



**More information:**

220-1002, Objective 4.5 - Environmental Impacts

<https://professormesser.link/1002040501>

**A11.** George, a sales manager, has recently replaced a broken mobile phone with a newer version. After receiving the new phone, he restored all of his apps and data from a recent backup. However, when he attempts to download any new email messages he receives a message, “Unable to decrypt email.” Which of the following steps should a technician follow to resolve this issue?

- A.** Install the latest operating system patches
  - B.** Delete the email app and reinstall
  - C.** Restart the phone
  - D.** Install the user's private keys
- 

**The Answer:** **D.** Install the user's private keys

A user's private keys are used to decrypt any messages that have been encrypted with the corresponding public keys. Installing these private keys onto the mobile device will allow the user to view their encrypted email messages.

**The incorrect answers:**

**A.** Install the latest operating system patches

Operating system updates would not provide any decryption functionality for email messages.

**B.** Delete the email app and reinstall

Fortunately, simply deleting an email app and reinstalling will not provide a method for reading encrypted messages. In this example, reinstalling the app would not resolve the current issue.

**C.** Restart the phone

Restarting the phone can solve many issues, but it won't get around email decryption issues. The only way to decrypt these messages is to install the proper decryption key on the phone.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

- A12.** The motherboard of a server in the corporate data center has started smoking, and flames can be seen inside the computer case. Which of the following would be the BEST way to extinguish this fire?
- A. An extinguisher with water
  - B. A foam-based extinguisher
  - C. Disconnect the power
  - D. A carbon dioxide extinguisher
- 

**The Answer:** D. A carbon dioxide extinguisher

For an electrical fire, it's best to use carbon dioxide, FM-200, or other dry chemicals to extinguish any flames.

**The incorrect answers:**

**A.** An extinguisher with water

Water and electricity don't go well together, and that applies just as strongly if a fire is involved.

**B.** A foam-based extinguisher

Foam-based extinguishers have a similar effect as a water extinguisher, and you shouldn't use them with electrical equipment.

**C.** Disconnect the power

Although it's important to disconnect the power source, the more important task will be to put out the fire. Removing the power source would not extinguish an electrical fire once it has started.



**More information:**

220-1002, Objective 4.4 - Safety Procedures

<https://professormesser.link/1002040401>

**A13.** Which of these Windows features provides full disk encryption for all data on a storage drive?

- A.** Domain Services
  - B.** EFS
  - C.** BranchCache
  - D.** BitLocker
- 

**The Answer:** **D.** BitLocker

BitLocker provides full disk encryption (FDE) for Windows operating system volumes.

**The incorrect answers:**

**A.** Domain Services

Windows Domain Services are used as a centralized database for management of large-scale Windows implementations. Domain Services itself is not an encryption mechanism.

**B.** EFS

EFS (Encrypting File System) is a feature of the NTFS (NT File System) that provides encryption at the file system level. Individual files and folders can be encrypted in Windows using EFS.

**C.** BranchCache

BranchCache is a technology that can minimize the use of slower wide area network links to remote sites. Files used often are kept onsite with BranchCache rather than transmitted over the wide area network.



**More information:**

220-1002, Objective 1.2 - Windows in the Enterprise  
<https://professormesser.link/1002010204>

**A14.** Which of the following governmental policies manages the use of personal data?

- A. PCI DSS
  - B. EULA
  - C. GDPR
  - D. FOSS
- 

**The Answer: C. GDPR**

GDPR (General Data Protection Regulation) is a European regulation that provides data protection and privacy for individuals in the European Union.

**The incorrect answers:**

**A. PCI DSS**

PCI DSS (Payment Card Industry Data Security Standard) is a set of guidelines for protecting credit card data. PCI DSS are industry guidelines and are not directly associated with governmental regulation.

**B. EULA**

EULA (End User Licensing Agreement) determines how software can be used by the end user. This agreement is not a governmental policy.

**D. FOSS**

FOSS (Free and Open Source) software is freely available and commonly includes the source code of the software. FOSS is not associated with a governmental policy.



**More information:**

220-1002, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1002040601>

**A15.** A user in the accounting department has recently installed a new app on their Android tablet. The app was not downloaded from the central app store, but instead was downloaded directly from a website as an .apk file. Which of the following would describe this installation process?

- A.** Cloud service
  - B.** Sideloaded
  - C.** Biometrics
  - D.** Encrypted
- 

**The Answer:** **B.** Sideloaded

Apps that are not downloaded from a central app store are called sideloaded apps. A good security best-practice is to use trusted app stores and to avoid sideloading any unknown or untrusted software.

**The incorrect answers:**

**A.** Cloud service

Cloud services would describe the use of an app or service that is located on an external device. Locally downloaded apps would not be described as a cloud service.

**C.** Biometrics

Biometrics describes measurements based on human characteristics, such as a fingerprint or facial recognition.

**D.** Encrypted

Android .apk files are not necessarily encrypted by default, and sideloading the file does not imply any level of cryptographic functionality.



**More information:**

220-1002, Objective 2.8 - Securing Mobile Devices

<https://professormesser.link/1002020801>

**A16.** A help desk technician has been given a network diagram that shows switch interfaces grouped by VLAN. Which of the following would BEST describe this documentation?

- A.** Logical diagram
  - B.** Knowledge base
  - C.** Inventory management
  - D.** Operational procedures
- 

**The Answer:** **A.** Logical diagram

A network VLAN (Virtual LAN) diagram is a logical view of a network configuration. A diagram that documented the individual switch interfaces would be a physical diagram.

**The incorrect answers:**

**B.** Knowledge base

A knowledge base is a database of processes, procedures, and technical troubleshooting steps. Network documentation is considered confidential information and would not commonly be stored in a knowledge base.

**C.** Inventory management

An inventory management system would include computer serial numbers, location information, asset tag numbers, and other physical inventory details. VLAN information would not commonly be stored in an inventory management database.

**D.** Operational procedures

It's always important to have a list of operational procedures, but storing VLAN information in a procedural document isn't a best practice.



**More information:**

220-1002, Objective 4.1 - Documentation Best Practices

<https://professormesser.link/1002040101>

- A17.** A system administrator is troubleshooting an older application on a Windows 10 computer and needs to modify the UAC process. Which of the following options would provide access to these settings?
- A.** Device Manager
  - B.** System Information
  - C.** Event Viewer
  - D.** User Accounts
- 

**The Answer:** **D.** User Accounts

UAC (User Account Control) settings are contained in the Control Panel's User Accounts applet.

**The incorrect answers:**

**A.** Device Manager

The Device Manager allows a user to enable, disable, and manage device drivers, but it doesn't provide any access to the UAC settings.

**B.** System Information

The System Information utility can provide information about a system's hardware, components, and software environment. UAC controls are not located in the System Information utility.

**C.** Event Viewer

The Event Viewer provides a consolidated view of all system logs, but it doesn't provide any access to the User Account Control settings.



**More information:**

220-1002, Objective 1.5 - Windows Administrative Tools

<https://professormesser.link/1002010501>

**A18.** An office power system occasionally experiences minor voltage spikes during the business day. Which of the following would be the BEST way to address this power issue?

- A. Power down when not actively working
  - B. Confirm that the building has an electrical ground
  - C. Connect a surge suppressor to each system
  - D. Maintain an inventory of replacement power supplies
- 

**The Answer:** C. Connect a surge suppressor to each system

A surge suppressor can help even out voltage spikes in an electrical system. It's common to use a surge suppressor at each workstation to limit the effect of these voltage spikes.

**The incorrect answers:**

**A.** Power down when not actively working

Although powering down a system would certainly protect it from voltage issues, it would not be a very efficient way of working.

**B.** Confirm that the building has an electrical ground

A good ground is an important part of any building's electrical system, but the ground won't help filter out the occasional voltage spike.

**D.** Maintain an inventory of replacement power supplies

If you don't use surge suppressors and you have constant power spikes, you might need replacement power supplies. However, it would be more effective to use surge suppressors instead of replacing power supplies.



**More information:**

220-1002, Objective 4.3 - Disaster Recovery

<https://professormesser.link/1002040301>

**A19.** What is the maximum amount of RAM supported by a 32-bit version of an operating system?

- A.** 4 GB
  - B.** 8 GB
  - C.** 16 GB
  - D.** 192 GB
- 

**The Answer:** **A.** 4 GB

The limited address space of a 32-bit operating system can only support 4 GB of system memory.

**The incorrect answers:**

**B.** 8 GB

A 32-bit operating system hits a limit at 4 GB of addressable memory. Although there are some techniques to work around this 4 GB limitation, they're not often implemented in practice.

**C.** 16 GB

4 GB is the limit for 32-bit operating systems.

**D.** 192 GB

192 GB would be well over the limit for 32-bit operating systems.



**More information:**

220-1002, Objective 1.1 - Operating Systems Overview

<https://professormesser.link/1002010101>

**A20.** Daniel, a user, is attempting to start an application on his laptop computer. Each time the application shows the starting graphic, it suddenly disappears and the application icon disappears from the taskbar. A technician would like to get more information about each previous occurrence of the application crash. Which of these choices would provide these details?

- A.** Event Viewer
  - B.** Task Manager
  - C.** Startup Repair
  - D.** Safe Mode
- 

**The Answer:** **A.** Event Viewer

Event Viewer contains a consolidated log of all system and application logs. A technician can use Event Viewer to review all past events on the system.

**The incorrect answers:**

**B.** Task Manager

Task Manager provides a real-time view of performance across many different system metrics, but it doesn't provide a way to review historical performance or events.

**C.** Startup Repair

Startup Repair is a useful tool when a system is not able to boot. Startup Repair does not resolve problems with applications that will not properly start.

**D.** Safe Mode

Safe Mode is useful for testing in a minimal operating system environment, but it doesn't provide any additional method of viewing application crash event logs.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues

<https://professormesser.link/1002030201>

**A21.** Which of the following would be unnecessary if a rainbow table is used?

- A. Spoofing
  - B. Social engineering
  - C. Brute force attack
  - D. DDoS
- 

**The Answer:** C. Brute force attack

A rainbow table is an optimized, pre-built set of hashes. Since the hashing calculation has already been completed, it's not necessary to brute force the original password from the hash. It simply takes a quick search through the rainbow table to quickly match a hash with a password.

**The incorrect answers:**

**A. Spoofing**

Spoofing is a technique where one device pretends to be another device. A rainbow table would not be associated with an attacker that is spoofing.

**B. Social engineering**

Social engineering is an attack method that uses many different psychological techniques to obtain access or information. A rainbow table is not part of a social engineering attack.

**D. DDoS**

DDoS (Distributed Denial of Service) is an attack type that uses many different and distributed systems to force a service to fail. A rainbow table is not used with a DDoS attack.



**More information:**

220-1002, Objective 2.5 - Brute Force Attacks

<https://professormesser.link/1002020505>

**A22.** A system administrator is upgrading an email service in the corporate data center. During the upgrade, an error message appears and the upgrade fails. Subsequent attempts to perform the upgrade also fail. Which of the following processes should the system administrator follow to return the email server to its previous state?

- A.** Backout plan
  - B.** Disaster recovery plan
  - C.** Incident response plan
  - D.** Power plan
- 

**The Answer:** **A.** Backout plan

Even with the best planning, there can always be unexpected events. Every planned change needs to have a backout plan to return the environment to its original state.

**The incorrect answers:**

**B.** Disaster recovery plan

A disaster recovery plan is written for major events that impact a large portion of an organization. An email upgrade that goes badly does not meet the scope of needing a disaster recovery plan.

**C.** Incident response plan

An incident response plan is commonly used to address a security event. Issues discovered during the planned upgrade of an email server would not be associated with an incident response plan.

**D.** Power plan

The Windows operating system allows users to modify the power use on their systems using built in power plans. These environmental controls are not associated with the change control process.



**More information:**

220-1002, Objective 4.2 - Change Management

<https://professormesser.link/1002040201>

**A23.** A user in the shipping department has opened a help desk ticket for problems found when browsing to certain Internet sites. The user also has slow access to other sites and difficulty sending and receiving emails from the local email server. A technician performs some basic troubleshooting and finds that CPU utilization is low, memory usage is minimal, and half of network pings return a response. Which of the following would be the best NEXT troubleshooting step?

- A.** Remove all startup applications and reboot the computer
  - B.** Restart in Safe Mode and repeat the tests
  - C.** Check the statistics on the user's switch port
  - D.** Scan with an anti-malware utility
- 

**The Answer:** **C.** Check the statistics on the user's switch port

The only significant issue that appeared during the diagnostics process is that half of the ping tests were rejected. Checking the switch statistics would likely provide some additional information about the issue.

**The incorrect answers:**

**A.** Remove all startup applications and reboot the computer

None of the CPU or memory checks appeared to show any issues with application use or resource utilization. There would be no immediate need to remove all startup applications or restart the system

**B.** Restart in Safe Mode and repeat the tests

The operating system does not appear to be restricting the access to other websites, so restarting in Safe Mode would not be the most likely next step in troubleshooting this issue.

**D.** Scan with an anti-malware utility

Although malware can certainly be a significant concern, there's nothing in the CPU or memory statistics that would show an immediate concern of malware.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1002030101>

**A24.** A system administrator has created a shared folder on a server to store operating system images. Technicians will access the shared folder to download the latest images when performing large-scale system installations. Which of the following will be the MOST likely method of accessing this data?

- A.** Map the shared folder to an available drive letter
  - B.** Download the shared folder through a proxy
  - C.** Link the images to a cloud storage service
  - D.** Access the folder using a remote access client
- 

**The Answer:** **A.** Map the shared folder to an available drive letter  
The easiest and most efficient way for technicians to access the drive share is to map a drive letter to the share and transfer the files directly.

**The incorrect answers:**

**B.** Download the shared folder through a proxy

There's no mention of a proxy in the question, and adding a proxy to this process would not provide any additional features or benefits.

**C.** Link the images to a cloud storage service

Operating system images are relatively large, and transferring them to an external cloud-based service would add additional time and bandwidth to resources that are already located on a local file server.

**D.** Access the folder using a remote access client

The installation of an operating system requires direct access to the installation files, and a remote access client would not provide direct access to the files.



**More information:**

220-1002, Objective 1.8 - Windows Network Technologies

<https://professormesser.link/1002010802>

**A25.** A desktop administrator is installing a 64-bit version of Windows 10 Pro on a workstation, but the installation will not start. The workstation configuration is:

- 1 GHz CPU
- 2 GB of RAM
- 15 GB of free storage space
- 1280 x 720 video resolution

Which of the following would allow this installation to proceed?

- A.** Increase free storage space to 20 GB
  - B.** Decrease resolution to 800 x 600
  - C.** Upgrade to a faster processor
  - D.** Increase RAM to 4 GB
- 

**The Answer:** **A.** Increase free storage space to 20 GB

Windows 10 x64 requires a minimum of 20 GB free storage space.

**The incorrect answers:**

**B.** Decrease resolution to 800 x 600

The only video requirement for the Windows 10 installation process is a Microsoft DirectX 9 graphics device with a WDDM driver.

**C.** Upgrade to a faster processor

The minimum supported processor to install Windows 10 is a 1 GHz CPU.

**D.** Increase RAM to 4 GB

The minimum RAM required to install Windows 10 x64 is 2 GB.



#### More information:

220-1002, Objective 1.2 - An Overview of Windows 10

<https://professormesser.link/1002010203>

**A26.** A security technician has identified malware that is running as part of the OS kernel. Traditional anti-malware scans were not able to identify any problems on the computer. Which of the following would be the BEST description of this malware?

- A. Rootkit
  - B. Worm
  - C. Botnet
  - D. Crypto-malware
- 

**The Answer: A. Rootkit**

A rootkit is a type of malware that modifies core system files and can be invisible to the operating system. In this example, malware that runs as part of the kernel and can't be seen by traditional anti-malware is a rootkit.

**The incorrect answers:**

**B. Worm**

A virus commonly needs a user to click on a file or to execute an application. A worm is a type of virus that doesn't need any human intervention and can self-replicate between systems.

**C. Botnet**

A botnet (robot network) is a group of computers that are under the control of a third-party. Botnets can be used to provide large-scale distributed attacks.

**D. Crypto-malware**

Crypto-malware is a broad categorization of malware that involves a cryptographic function. One common type of crypto-malware is ransomware that encrypts your files and holds them for a cash ransom.



**More information:**

220-1002, Objective 2.4 - Types of Malware  
<https://professormesser.link/1002020401>

**A27.** A help desk technician has been called to a training room that uses Android tablets as presentation devices. An application used for the training program will not start on any of the tablets. When the application is selected, the splash screen appears for a moment and then completely disappears with no error message. Which of the following would be the best NEXT troubleshooting step?

- A.** Install all operating system updates
  - B.** Uninstall the application
  - C.** Power cycle the tablets
  - D.** Roll back to the previous application version
- 

**The Answer:** **C.** Power cycle the tablets

Before making any changes to the operating system or application software, it would be useful to know if power cycling the tablets would have an effect. If the symptom was to disappear after the restart, then no immediate changes would be required.

**The incorrect answers:**

**A.** Install all operating system updates

Making a change to the system without understanding the issue would be a blind guess. It would be a better practice to gather more information about the problem before making changes.

**B.** Uninstall the application

Uninstalling the application would make it very difficult to troubleshoot the application, and it's not the best possible option before gathering more information about the problem.

**D.** Roll back to the previous application version

A technician wouldn't want to make significant changes to the application or the operating system until they knew more about the problem and tried to resolve the issue without installing or uninstalling any software.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**A28.** A user on the headquarters network has opened a help desk ticket about their Windows desktop. When starting their computer, the login process proceeds normally but the Windows desktop takes fifteen minutes to appear. Yesterday, the desktop would appear in just a few seconds. Which of the following would be the MOST likely reason for this issue?

- A.** Slow profile load
  - B.** Incorrect boot device order
  - C.** Faulty RAM
  - D.** Incorrect username and password
- 

**The Answer:** **A.** Slow profile load

A roaming user profile is commonly used on enterprise Windows networks to allow a user's desktop to follow them to any computer. When a user logs in, their profile is downloaded to the local computer. If there is any network latency to the domain controller, the login process could be significantly slower.

**The incorrect answers:**

**B.** Incorrect boot device order

A BIOS setting of an incorrect boot device order would cause the computer to boot a completely different operating system or no operating system at all. This would not be associated with a slow login process.

**C.** Faulty RAM

Faulty RAM would cause the system to fail or crash. Bad RAM would not commonly cause a login process to perform slowly.

**D.** Incorrect username and password

Incorrect login credentials would present an error message instead of slowing down the login process.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1002030101>

**A29.** A system administrator has been asked to install a new application on a server, but the application is 64-bit and the server operating system is 32-bit. Which of the following describes the issue associated with this installation?

- A.** File permissions
  - B.** OS compatibility
  - C.** Installation method
  - D.** Available drive space
- 

**The Answer:** **B.** OS compatibility

Although 32-bit applications will run on a 64-bit operating system, the reverse is not true. A 64-bit application will require a 64-bit operating system to work.

**The incorrect answers:**

**A.** File permissions

File permissions between a 32-bit operating system and a 64-bit operating system are effectively identical.

**C.** Installation method

There isn't any significant difference when installing an application on a 32-bit operating system or a 64-bit operating system.

**D.** Available drive space

Although there will be a slight difference in drive space requirements between a 32-bit application and a 64-bit application, the differences would not be enough to cause an issue with free drive space.



**More information:**

220-1002, Objective 1.7 - Installing Applications

<https://professormesser.link/1002010701>

**A30.** A security guard has reported that a person was seen passing through a secure door without using a door badge. The intruder slipped through the door by closely following the person in front of them. Which of these would best describe these actions?

- A.** Dumpster diving
  - B.** Brute force
  - C.** Phishing
  - D.** Tailgating
- 

**The Answer:** **D.** Tailgating

Using someone else to gain access to a building or through a locked door is tailgating.

**The incorrect answers:**

**A.** Dumpster diving

An attacker that digs through an outdoor trash bin is a dumpster diver. Digging through the garbage does not allow access through a secure door.

**B.** Brute force

A brute force attack is a software attack that attempts many different combinations until the original data is discovered. A brute force attack is not a physical attack against locked doors or restricted areas.

**C.** Phishing

Phishing is a method of coercing private information from unsuspecting individuals. This process commonly uses a combination of social engineering and spoofing.



**More information:**

220-1002, Objective 2.5 - Social Engineering Attacks

<https://professormesser.link/1002020501>

**A31.** A Linux administrator needs to create a system image of a laptop used by the help desk for network troubleshooting. Which of the following utilities would provide this functionality?

- A.** dd
  - B.** sudo
  - C.** ifconfig
  - D.** apt-get
- 

**The Answer:** **A.** dd

The Linux dd command is used to copy and convert files. It's commonly used to backup and restore an entire Linux partition as a disk image.

**The incorrect answers:**

**B.** sudo

The sudo command allows a Linux user to execute a command as the superuser or as any other user on the system. The sudo command on its own does not provide any backup or imaging functionality.

**C.** ifconfig

The Linux ifconfig command is similar in function to the Windows ipconfig command. The output of ifconfig will display network interface and IP address configuration details.

**D.** apt-get

The Linux apt-get is an Advanced Packaging Tool command that handles the management of application packages on the system.



**More information:**

220-1002, Objective 1.9 - Basic Linux Commands

<https://professormesser.link/1002010906>

**A32.** An internal audit has found that a server in the DMZ has been participating in DDoS attacks against external devices. What type of malware would be MOST likely found on this server?

- A. Worm
  - B. Rootkit
  - C. Keylogger
  - D. Spyware
  - E. Botnet
- 

**The Answer:** E. Botnet

A botnet (robot network) is a collection of systems that are under the control of a third-party. It's common for those controlling the botnet to use them for DDoS (Distributed Denial-of-Service) or other large-scale network tasks.

**The incorrect answers:**

**A. Worm**

A worm is a type of malware that can replicate between systems without any human intervention. A worm would not commonly participate in a DDoS attack

**B. Rootkit**

A rootkit is a type of malware that modifies core system files and is often invisible to the operating system. A system participating in a DDoS would not commonly be categorized as a rootkit.

**C. Keylogger**

A keylogger will store all of the input made from a keyboard and transmit this information to a third-party. The attacker will commonly use these logged keystrokes to gain unauthorized access to other sites.

**D. Spyware**

Spyware is a type of malware that monitors browsing locations, captures keystrokes, and watches user activity.



**More information:**

220-1002, Objective 2.4 - Types of Malware

<https://professormesser.link/1002020401>

**A33.** A user has delivered a broken laptop to the help desk, and he's visibly upset and quite vocal about the problem he's having. He's also asking for a very specific repair that doesn't appear to have any relationship to his issue. What's the best way to handle this situation?

- A.** Repeat your understanding of the issue to the customer and provide an estimate and follow-up time
  - B.** Refuse the repair until the customer calms down
  - C.** Inform the customer of his mistake with the proposed repair
  - D.** Refuse to make any commitments until the computer is examined
- 

**The Answer:** **A.** Repeat your understanding of the issue to the customer and provide an estimate and follow-up time

The best response in a stressful situation is to listen, ask questions, and refrain from arguing or acting defensive. In this situation, the technician should gather as much information about the problem and keep all responses focused on resolving the problem.

**The incorrect answers:**

**B.** Refuse the repair until the customer calms down

It's always preferable to avoid any comments that would be associated with emotion. Technical problems can be stressful enough on their own, and adding additional stress is not going to help repair the system.

**C.** Inform the customer of his mistake with the proposed repair

This isn't a game, and there are no winners or losers. The technician will be left to resolve the issue, regardless of the root cause. It's not necessary to comment or speculate on any proposed repair process.

**D.** Refuse to make any commitments until the computer is examined

The technician is ultimately responsible for resolving the issue, and it would help everyone involved to maintain a constant line of communication.



**More information:**

220-1002, Objective 4.7 - Professionalism

<https://professormesser.link/1002040702>

**A34.** Daniel, a user in the finance department, has purchased a new Android smartphone and has installed a number of productivity apps. After a day of use, Daniel finds that the battery is draining rapidly, even when the phone is not being used. Which of the following tasks should Daniel perform after completing a factory reset?

- A. Disable Bluetooth
  - B. Check app sharing permissions
  - C. Run a speed test on the cellular connection
  - D. Scan each app before installation
- 

**The Answer:** D. Scan each app before installation

An App scanner can provide information about the legitimacy and functionality of an app before it is installed onto a mobile device. Before an unknown app is installed, it's always a best practice to gather as much information as possible. In this example, it's likely that one of the apps installed onto the phone was using more resources and battery life than a typical app.

**The incorrect answers:**

**A.** Disable Bluetooth

Given the limited information in the question, there's no evidence that Bluetooth was related to any of the battery issues on this smartphone.

**B.** Check app sharing permissions

Sharing permissions can limit an app's access to personal data, but it would not cause the battery to drain faster than normal.

**C.** Run a speed test on the cellular connection

The speed of a cellular network connection would not have a significant impact on the battery life of a smartphone.



**More information:**

220-1002, Objective 3.5

Troubleshooting Mobile Device Security

<https://professormesser.link/1002030501>

**A35.** A network administrator has configured all of their wireless access points with WPA2 security. Which of the following technologies would be associated with this configuration?

- A.** RC4
  - B.** TACACS
  - C.** TKIP
  - D.** AES
- 

**The Answer: D. AES**

AES (Advanced Encryption Standard) is the encryption algorithm used in WPA2 (Wi-Fi Protected Access version 2).

**The incorrect answers:**

**A. RC4**

The first version of WPA used RC4 (Rivest Cipher 4) to encrypt wireless traffic.

**B. TACACS**

TACACS (Terminal Access Controller Access-Control System) is an authentication protocol used to control access to network resources. TACACS is not part of the WPA2 protocol.

**C. TKIP**

TKIP (Temporal Key Integrity Protocol) is the underlying security protocol used in the initial WPA encryption standard.



**More information:**

220-1002, Objective 2.3 - Wireless Security

<https://professormesser.link/1002020301>

**A36.** A user has reported that all Google search results in their Internet browser are displaying a non-Google website. This redirection occurs each time a Google search is attempted. Which of the following would be the BEST way to prevent this issue in the future?

- A.** Windows Firewall
  - B.** MAC filtering
  - C.** Port security
  - D.** Certificate-based authentication
  - E.** Anti-malware utility
- 

**The Answer:** **E.** Anti-malware utility

A browser hijack is a very specific attack type that is commonly the result of a malware infection.

**The incorrect answers:**

**A.** Windows firewall

The Windows firewall is useful for preventing inbound connections, but most malware is installed by the user. This installation process circumvents the firewall and it's the reason we rely on both a firewall and anti-malware software.

**B.** MAC filtering

MAC filtering is commonly used on a network device to limit which devices can communicate on a network. MAC filtering would not be related to a browser hijack.

**C.** Port security

Port security prevents unauthorized users from connecting to a switch interface. Port security is not associated with a browser hijack.

**D.** Certificate-based authentication

Certificate-based authentication provides a method to verify a user during the authentication process. This authentication mechanism is not related to browser hijacking.



**More information:**

220-1002, Objective 2.2 - Logical Security

<https://professormesser.link/1002020201>

**A37.** A user has installed multiple applications over the last week. During the startup process, the computer now takes over fifteen minutes to display the Windows desktop. Which of the following utilities would help the system administrator troubleshoot this issue?

- A.** defrag
  - B.** dism
  - C.** msconfig
  - D.** robocopy
- 

**The Answer:** **C.** msconfig

The msconfig (System Configuration) command is useful for managing the startup process of services. Prior to Windows 8.1, System Configuration can also be used to manage applications during the startup process.

**The incorrect answers:**

**A. defrag**

Although a fragmented drive can cause minor inefficiencies when accessing data, it would not cause a system delay of over fifteen minutes during the boot process.

**B. dism**

The dism (Deployment Image Servicing and Management) utility allows the administrator to manage Windows Imaging Format (WIM) files. The delays occurring on this system do not appear to be related to any issue with a system image.

**D. robocopy**

Robocopy (Robust Copy) is an advanced copy utility that can be used to transfer files between folders or systems. The robocopy utility would not provide any significant troubleshooting assistance with this slowdown issue.



**More information:**

220-1002, Objective 1.5 - System Configuration

<https://professormesser.link/1002010503>

**A38.** A server administrator is replacing the memory in a database server. Which of the following steps should be followed FIRST?

- A.** Remove the existing memory modules
  - B.** Wear an air filter mask
  - C.** Disconnect all power sources
  - D.** Connect an ESD strap
- 

**The Answer:** **C.** Disconnect all power sources

The first step when working inside of a computer or printer is to remove all power sources.

**The incorrect answers:**

**A.** Remove the existing memory modules

Prior to removing the existing modules, the power source would need to be disconnected and an ESD strap would need to be attached to the computer case.

**B.** Wear an air filter mask

A filtered mask would not commonly be required for replacing memory modules. If the environment is very dusty or dirty, then a filtered mask may be necessary.

**D.** Connect an ESD strap

An ESD (Electrostatic Discharge) strap would allow the technician to minimize the potential of an electrostatic discharge. However, disconnecting the power source takes a higher priority.



**More information:**

220-1002, Objective 4.4 - Safety Procedures

<https://professormesser.link/1002040401>

**A39.** A technician is dismantling a test lab for a recently completed project, and the lab manager would like to use the existing computers on a new project. However, the security administrator would like to ensure that none of the data from the previous project is accessible on the existing hard drives. Which of the following would be the best way to accomplish this?

- A.** Quick format
  - B.** Degauss the drives
  - C.** Regular format
  - D.** Reinstall the operating system
- 

**The Answer:** **C.** Regular format

A standard Windows format with the regular formatting option overwrites each sector of the drive with zeros. After this format is complete, the previous data on the drive is unrecoverable.

**The incorrect answers:**

**A.** Quick format

A standard Windows format with the quick format option clears the master file table, but it doesn't overwrite any data on the drive. With the right software, the previous data could be recovered.

**B.** Degauss the drives

Degaussing the drives would remove the magnetic fields necessary for the drives to work properly. Although this would make the previous data unrecoverable, it would also cause the hard drives to be unusable.

**D.** Reinstall the operating system

Reinstalling the operating system may not overwrite any of the previous user data on the drive. Recovery software would be able to identify and "undelete" the previous drive data.



**More information:**

220-1002, Objective 2.9 - Data Destruction and Disposal

<https://professormesser.link/1002020901>

**A40.** A system administrator needs to view a set of application log files contained in a folder named "logs." Which of the following commands should be used to make this the current active directory?

- A.** cd logs
  - B.** mv logs
  - C.** dir logs
  - D.** md logs
- 

**The Answer:** **A.** cd logs

The "cd" command is short for change working directory, and it can be used in Windows or Linux to move around the file system.

**The incorrect answers:**

**B.** mv logs

The mv command is commonly used in Linux to "move" a file from one place to another, or to rename an existing file from one name to another.

**C.** dir logs

The dir (directory) command will list files and directories in a folder. If the command specifies additional text, then the results will be filtered for that specific text.

**D.** md logs

The Windows md command is an abbreviation of the mkdir (make directory) command. The md command will create a folder in the file system.



**More information:**

220-1002, Objective 1.4 - Microsoft Command Line Tools  
<https://professormesser.link/1002010401>

**A41.** Which of the following technologies would be the best choice to boot computers in a training room over the network?

- A. MBR
  - B. NTFS
  - C. Dual boot
  - D. PXE
- 

**The Answer: D. PXE**

PXE or "Pixie" (Preboot eXecution Environment) is a method of booting a computer from a device over the network instead of from operating system files on a local storage device. This method is especially useful when managing large groups of devices, such as a training room.

**The incorrect answers:**

**A. MBR**

MBR (Master Boot Record) describes the information contained on the first sector of a drive. MBR is not used to boot devices across the network.

**B. NTFS**

NTFS (NT File System) is a file system designed for Windows computers. Although a system may store files using NTFS, the file system does not include any features that would allow it to be booted over the network.

**C. Dual boot**

A dual boot system contains a storage device with multiple operating systems, and each operating system can be individually selected and booted when starting the computer.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**A42.** Which of these OS installation types uses an XML file that answers all of the questions normally provided during the installation?

- A. Unattended
  - B. Image
  - C. PXE
  - D. Clean
- 

**The Answer:** A. Unattended

An unattended Windows installation requires the administrator to answer the normal installation questions in a single XML file. This allows the installation process to continue from the beginning to end without any user intervention.

**The incorrect answers:**

**B. Image**

A system image is a complete backup of a volume or drive. The process for installing a system image is to copy the entire contents of the image to the drive of the computer. The normal operating system setup is not used, so an XML file would not answer installation questions.

**C. PXE**

PXE, or "Pixie," (Preboot eXecution Environment) is a method of booting a computer across the network. Booting with PXE does not answer files during an operating system installation.

**D. Clean**

A clean install is used to completely replace an existing operating system with a fresh version. Although this can be used with an unattended answer file, a clean installation by itself does not include an XML file with answers to installation questions.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**A43.** A user has noticed that their system has been running very slowly over the last few days. They have also noticed files stored on their computer randomly disappear after the files are saved. The user has rebooted the computer, but the same problems continue to occur. Which of the following should the user perform to resolve these issues?

- A.** Boot to Safe Mode
  - B.** Release and renew the network connection
  - C.** Install anti-malware software
  - D.** Upgrade the system RAM
- 

**The Answer:** **C.** Install anti-malware software

A system that's running slowly and has files that randomly disappear are clear indications of malware. The best step to follow would be the installation of anti-malware software to identify and hopefully remove any existing malware from the system.

**The incorrect answers:**

**A. Boot to Safe Mode**

Booting to Safe Mode might be a troubleshooting step during the malware removal phase, but it won't commonly stop malware from exhibiting the symptoms identified in the question.

**B. Release and renew the network connection**

Releasing and renewing the network connection will cause the DHCP (Dynamic Host Configuration Protocol) assignment process to complete, but that won't resolve any issues with slowdowns and files disappearing.

**D. Upgrade the system RAM**

Upgrading the RAM might address slowdown issues, but it wouldn't resolve any problems related to files randomly disappearing from the storage drive.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues

<https://professormesser.link/1002030201>

**A44.** A user in the sales department has opened a help desk ticket to report a dim display on their tablet. When they use the tablet in the office, the screen brightness is normal. In meetings with customers, the display appears much dimmer. Which of these would be the MOST likely reason for this difference?

- A. The tablet display is faulty
  - B. The tablet is brighter when connected to power
  - C. The tablet backlight is on a timer
  - D. Indoor LED lighting is causing the display to dim
- 

**The Answer:** B. The tablet is brighter when connected to power

The power profiles on the tablet are most likely configured to provide a brighter backlight when connected to a power source. Since the backlight uses relatively large amounts of the battery, it's often configured to be dimmer when not connected to a power source.

**The incorrect answers:**

A. The tablet display is faulty

The display is working properly when connected to power, so the issue would most likely not be related to faulty display hardware.

C. The tablet backlight is on a timer

The tablet backlight appears to be changing based on the availability of a power source rather than a timer or time of day.

D. Indoor LED lighting is causing the display to dim

Although many tablets can change their brightness based on ambient light, the LED lighting would not cause a tablet display to dim more than other lighting types.



#### More information:

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**A45.** The hard drive in a macOS desktop has failed and none of the data on the drive was recoverable. A new storage drive has now been installed. Which of the following should be used to restore the data on the computer?

- A.** Backup and Restore
  - B.** Boot Camp
  - C.** Time Machine
  - D.** Disk Utility
- 

**The Answer: C. Time Machine**

The build-in backup and restore utility in macOS is appropriately called Time Machine.

**The incorrect answers:**

**A. Backup and Restore**

The Windows operating system includes its own backup and restore utility literally called "Backup and Restore."

**B. Boot Camp**

Boot Camp is the utility that allows the macOS operating system to dual-boot to a Windows operating system.

**D. Disk Utility**

Disk Utility is a macOS tool that allows the user to view, modify, and manage storage drives.



**More information:**

220-1002, Objective 1.9 - macOS Tools

<https://professormesser.link/1002010902>

**A46.** A user purchased a copy of home tax software and has installed it on their company computer. This morning, the user logs in and finds that the tax software has been automatically removed from the system. Which of the following would be the MOST likely reason for this result?

- A. The company per-seat licenses are all in use
  - B. The software uses a FOSS license
  - C. The user has installed a personal license
  - D. The software is subject to the GDPR
- 

**The Answer:** C. The user has installed a personal license

Personally licensed software can be difficult to audit on computers that are owned by a company, and many organizations will not allow software to be installed on company-owned systems if the company has not purchased the license.

**The incorrect answers:**

A. The company per-seat licenses are all in use

This home tax software is not owned by the company, so the company would not have per-seat licenses to distribute.

B. The software uses a FOSS license

A FOSS (Free and Open Source) license would not cause any licensing issues, and many companies will install FOSS software on their systems.

D. The software is subject to the GDPR

The GDPR (General Data Protection Regulation) are rules in the European Union that are specific to a user's control of their personal data. The GDPR regulations would not be the most likely reason for removing this software.



#### More information:

220-1002, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1002040601>

**A47.** A system administrator is upgrading four workstations from Windows 8.1 to Windows 10. All of the user files and applications are stored on the server, and no documents or settings need to be retained between versions. Which of these installation methods would be the BEST way to provide this upgrade?

- A.** Factory reset
  - B.** Repair installation
  - C.** Clean install
  - D.** Multiboot
- 

**The Answer:** **C.** Clean install

A clean install of Windows 10 will completely delete the previous operating system and install a new installation of the Windows 10 operating system. The previous Windows 8.1 operating system will no longer be available on the computer.

**The incorrect answers:**

**A.** Factory reset

A factory reset will restore the computer to the configuration from the original purchase. In this example, the factory reset will refresh the existing Windows 8.1 installation (or a previous version), instead of installing Windows 10.

**B.** Repair installation

A repair installation installs the current version of the operating system over itself in an effort to repair files that may have been deleted or damaged. This repair installation will not upgrade an operating system to a newer version.

**D.** Multiboot

A multiboot system will have multiple operating systems installed, and the user can choose the operating system during the boot process. In this scenario, the user would like to upgrade to Windows 10 and there is no requirement to maintain a Windows 8.1 installation.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**A48.** A computer on a manufacturing floor has been identified as a malware-infected system. Which of the following should be the best NEXT step to resolve this issue?

- A.** Disconnect the network cable
  - B.** Perform a malware scan
  - C.** Disable System Restore
  - D.** Download the latest anti-malware signatures
- 

**The Answer:** **A.** Disconnect the network cable

After identifying a system that may be infected with malware, it's important to quarantine that system and restrict any access to the local network or devices. Disconnecting the network cable would be an important step during the quarantine process.

**The incorrect answers:**

**B.** Perform a malware scan

Although a malware scan should eventually be performed, it's more important to limit the scope of the malware by quarantining the system.

**C.** Disable System Restore

The System Restore feature makes it easy to restore from a previous configuration, but it also makes it easy for malware to reinfect a system. Although it's important to disable System Restore to remove the restore points, it's more important to quarantine the system to prevent the spread of any malware.

**D.** Download the latest anti-malware signatures

Before scanning for malware, it's important to use the latest signatures. However, it's more important that the computer is quarantined to prevent the spread of any potential malware.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**A49.** A technician has been called to resolve an issue with a networked laser printer that is not printing. When the technician arrives on-site, they find the printer will require a hardware replacement. All hardware is managed by a third-party and will take a week before the printer is operational again. Which of the following would be the technician's best NEXT step?

- A.** Work on the next ticket in the queue
  - B.** Add a follow-up event for one week later
  - C.** Inform the user of the repair status
  - D.** Order a printer maintenance kit
- 

**The Answer:** **C.** Inform the user of the repair status

One of the most important skills for any technician is communication. Information about the delays should be shared with the customer, and the customer can then decide how they might want to proceed.

**The incorrect answers:**

**A.** Work on the next ticket in the queue

Before moving on, it's important to inform everyone involved of the current status and recommend any workarounds while waiting on the replacement hardware.

**B.** Add a follow-up event for one week later

It's certainly important to follow-up on this hardware replacement, but it's more important that the customer is informed of the plans going forward.

**D.** Order a printer maintenance kit

There's no mention in this question that the printer needs maintenance, although it would certainly be a good time to perform one if needed. However, it's more important to keep the customer informed of the status of their printer repair.



#### More information:

220-1002, Objective 4.7 - Communication

<https://professormesser.link/1002040701>

**A50.** An administrator is upgrading a Windows 8.1 Enterprise x64 computer to Windows 10. The user would like to maintain all applications and files during the upgrade process. Which of the following upgrade options would meet this requirement?

- A. Windows 10 Enterprise x86
  - B. Windows 10 Pro x64
  - C. Windows 10 Enterprise x64
  - D. Windows 10 Pro x86
- 

**The Answer:** C. Windows 10 Enterprise x64

A Windows upgrade that maintains applications and settings requires the destination version to be the same Windows edition or higher. Since the original Windows 8.1 is the Enterprise edition, the Windows 10 edition should also be the Enterprise version. It's also not possible to upgrade from a 32-bit version to 64-bit (or vice versa), so the Windows 10 operating system needs to be the x64 version.

**The incorrect answers:**

**A.** Windows 10 Enterprise x86

A 64-bit operating system cannot upgrade to a 32-bit version (or vice versa).

**B.** Windows 10 Pro x64

Since the starting Windows 8.1 edition is the Enterprise version, the final operating system must also be the same or higher. Windows 10 Pro is not the same or higher edition as Windows 8.1 Enterprise edition.

**D.** Windows 10 Pro x86

As with option B, the Pro edition of Windows 10 is not the same or higher edition as Windows 8.1 Enterprise.



**More information:**

220-1002, Objective 1.3 - Installing and Upgrading Windows  
<https://professormesser.link/1002010302>

**A51.** A user in the marketing department is using an application that randomly shuts down during normal use. When the problem occurs, the application suddenly disappears and no error messages are shown on the screen. Which of the following would provide the system administrator with additional information regarding this issue?

- A.** System Configuration
  - B.** Event Viewer
  - C.** Device Manager
  - D.** Local Security Policy
  - E.** SFC
- 

**The Answer:** **B.** Event Viewer

The Windows Event Viewer can provide extensive logs and information about the system and the applications running in Windows.

**The incorrect answers:**

**A.** System Configuration

The System Configuration utility can provide an easy interface to modify boot settings and services, but it won't provide any additional details about this application problem.

**C.** Device Manager

The Device Manager is used to control and manage hardware and device drivers. Device Manager doesn't contain any detailed information about problematic applications.

**D.** Local Security Policy

The Windows Local Security Policy can be used to configure password settings and login requirements, but it doesn't provide any detailed application troubleshooting information.

**E.** SFC

SFC (System File Checker) is used to verify that the core operating system files are valid. Application information isn't part of the SFC utility.



**More information:**

220-1002, Objective 1.5 - Windows Administrative Tools

<https://professormesser.link/1002010501>

**A52.** A workstation on a manufacturing floor is taking much longer than normal to boot. Which of the following would be the BEST way to troubleshoot this issue?

- A.** Replace the CPU
  - B.** Disable the startup applications
  - C.** Upgrade the RAM
  - D.** Install the latest OS patches
- 

**The Answer:** **B.** Disable the startup applications

Delays during the boot process can be caused by many issues, but a device that was previously working properly most likely has been changed. A single application install can create issues, so disabling startup applications would be an easy way to remove those from the troubleshooting process.

**The incorrect answers:**

**A.** Replace the CPU

If the CPU was faulty, the computer would most likely not be operational.

**C.** Upgrade the RAM

Upgrading RAM can often resolve application performance issues, but this computer was previously working with the existing amount of memory.

**D.** Install the latest OS patches

It's possible that problems might occur after an OS patch update, but it would not be most likely that these issues would occur prior to patching. Without knowing more about the issue, it would not be a best practice to make such a significant change to the system.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1002030101>

**A53.** A Windows 10 user is installing a new application that also installs a service. Which of the following permissions will be required for this installation?

- A.** Guest
  - B.** Power User
  - C.** Administrator
  - D.** Standard user
- 

**The Answer:** **C.** Administrator

The Administrator account is the superuser of a Windows device. If an installation needs to modify system files or install a service, then Administrator access will be required.

**The incorrect answers:**

**A.** Guest

The Guest account has very limited access to the system. A guest account cannot install applications or make any changes to the system, and the Guest account is usually disabled by default.

**B.** Power User

The legacy "Power User" permissions were removed from Windows 7 and later versions, so the Power User would have similar rights as a standard user.

**D.** Standard user

The standard user permissions would allow the installation of simple applications, but any changes to the operating system or services would require Administrator access.



**More information:**

220-1002, Objective 2.6 - Windows Security Settings

<https://professormesser.link/1002020601>

**A54.** A user working from home is not able to print to a laser printer at the corporate office. Which of the following would be the MOST likely reason for this issue?

- A.** DLP policy
  - B.** Outdated anti-virus signatures
  - C.** Disconnected VPN
  - D.** MDM configuration
- 

**The Answer: C. Disconnected VPN**

Remote users will commonly connect to the corporate office over a VPN (Virtual Private Network). This VPN is an encrypted tunnel that ensures that all traffic between the locations is protected from anyone monitoring the connection. If the VPN link is not active, then the remote user will be unable to use any resources at the corporate office.

**The incorrect answers:**

**A. DLP policy**

DLP (Data Loss Prevention) policies are designed to monitor network communication and prevent the transmission or storage of sensitive information such as credit card numbers or social security numbers. A DLP policy would not commonly be part of a printing problem.

**B. Outdated anti-virus signatures**

Anti-virus signatures would not commonly restrict the printing process, and the age of the signatures would only affect the ability of the anti-virus software to block known viruses.

**D. MDM configuration**

An MDM (Mobile Device Manager) is used to manage mobile tablets and phones. MDM configurations would not commonly have an impact on home users connecting to a corporate printer.



**More information:**

220-1002, Objective 2.2 - Logical Security

<https://professormesser.link/1002020201>

**A55.** An employee has modified the NTFS permissions on a local file share to provide read access to Everyone. However, users connecting from a different computer do not have access to the file. Which of the following is the reason for this issue?

- A. The NTFS permissions were not synchronized
  - B. Share permissions restrict access from remote devices
  - C. The user is an Administrator
  - D. Remote users are connecting with Guest accounts
- 

**The Answer:** **B.** Share permissions restrict access from remote devices  
NTFS (NT File System) permissions are used to control access from both local users and users over the network. For users connected over the network, the Windows share permissions are also used to determine access. If access is available locally but not across the network, then it's likely that the share permissions have additional access restrictions.

**The incorrect answers:**

**A.** The NTFS permissions were not synchronized

NTFS does not require any permissions to be synchronized or copied between systems.

**C.** The user is an Administrator

A Windows Administrator would not commonly be restricted from accessing local files, but this issue is not related to the local NTFS permissions. Since the access problems are for users across the network, the share permissions would most likely be the issue.

**D.** Remote users are connecting with Guest accounts

All remote access is managed through Windows share permissions. These share permissions, combined with the NTFS permissions, determine the rights that remote users will have to the resources.



**More information:**

220-1002, Objective 2.6 - Windows Security Settings

<https://professormesser.link/1002020601>

**A56.** A healthcare company has replaced some of their desktop computers with laptops and will be disposing of the older computers. The security administrator would like to guarantee that none of the existing data on the hard drives could be recovered once the systems are sent to the recycling center. Which of the following methods would meet this requirement?

- A.** Quick format
  - B.** Reinstall the OS
  - C.** Remove all user folders
  - D.** Shred the drives
- 

**The Answer:** **D.** Shred the drives

Of the available choices, the only option that would guarantee all data would be unrecoverable would be to physically destroy the drives in a shredder.

**The incorrect answers:**

**A.** Quick format

A quick format simply clears the index and does not overwrite any of the data on the drive. Recovery software would be able to restore data from a quick formatted drive.

**B.** Reinstall the OS

Reinstalling the operating system does not necessarily overwrite all data on the hard drive. Any data not overwritten could potentially be restored with recovery software.

**C.** Remove all user folders

Removing user folders with the normal Windows delete does not overwrite the section of the drive that contained the data. User folder data could possibly be restored with the use of recovery software.



**More information:**

220-1002, Objective 2.9 - Data Destruction and Disposal  
<https://professormesser.link/1002020901>

- A57.** A technician has been assigned a support ticket that urgently requests a laptop repair, but there are already many open support tickets ahead of this request. The technician doesn't recognize the name associated with the ticket. Which of these choices would be the best path to take?
- A.** Place the ticket into the queue as first-come, first-served
  - B.** Prioritize the support tickets by device type
  - C.** Triage the queue and prioritize the tickets in order of repair complexity
  - D.** Contact the end-user and determine the urgency of the repair
- 

**The Answer:** **D.** Contact the end-user and determine the urgency of the repair  
A support ticket marked as "urgent" should be evaluated to determine the timeframe for resolving the issue and the complexity of the task. If the end user feels that the issue is time-sensitive, then it's important to contact them and see what options might be available to get them up and running as quickly as possible.

**The incorrect answers:**

**A.** Place the ticket into the queue as first-come, first-served

Not all support tickets have the same priority, and it's the responsibility of the technician to properly triage the cases to handle the most critical first. It will usually involve some communication with the client to determine the scope of the issue.

**B.** Prioritize the support tickets by device type

The urgency of a technical issue isn't determined by the type of the device. Instead, the priority of issues should be based on the needs of the end user and the importance of their task.

**C.** Triage the queue and prioritize the tickets in order of repair complexity  
The complexity of a repair doesn't consider the importance of the repair to the organization's goals and objectives. An executive going into an important presentation may have a simple problem, but their issue has greater importance to the organization.



**More information:**

220-1002, Objective 4.7 - Communication

<https://professormesser.link/1002040701>

**A58.** A user has received a pop up message on their computer that states applications on their computer are infected with a virus. A technician has determined that the pop up message is a hoax that needs to be removed from the computer. The technician has disabled System Restore to remove all previous restore points. Which of the following tasks would be the best NEXT step?

- A.** Update the anti-virus signatures
  - B.** Educate the end-user
  - C.** Schedule anti-virus scans for midnight each day
  - D.** Boot the system with a pre-installation environment
- 

**The Answer:** **A.** Update the anti-virus signatures

After disabling system restore, the next step in virus removal is to remediate the system. To remove the malware, it's important the technician is using the latest set of signatures.

**The incorrect answers:**

**B.** Educate the end-user

This is one of the most important tasks for malware removal, but it's usually reserved for the final step when there's no longer any urgency to remove the malware.

**C.** Schedule anti-virus scans for midnight each day

Once the virus is removed, the system should be configured for on-demand scanning and additional scans each day. However, this would not immediately follow the disabling of System Restore.

**D.** Boot the system with a pre-installation environment

A pre-installation environment may be required for more difficult virus removal tasks, but this would only occur after the latest anti-virus signatures were downloaded and installed.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**A59.** A network administrator needs to manage a switch and firewall at a remote location. Which of the following would be the BEST choice for this requirement?

- A.** RDP
  - B.** Telnet
  - C.** SSH
  - D.** VNC
- 

### **The Answer: C. SSH**

SSH (Secure Shell) provides encrypted console communication, and it's commonly used to manage devices across the network. If an administrator is managing a server, switch, router, or firewall, they're probably using SSH.

### **The incorrect answers:**

#### **A. RDP**

Microsoft RDP (Remote Desktop Protocol) is commonly used to share the desktop of a Windows computer. Most switches and firewalls are not Windows devices, so RDP would not be the best choice for this connection.

#### **B. Telnet**

Telnet (Telecommunication Network) is very similar to SSH, but Telnet does not use encrypted communication. Because Telnet traffic is sent in the clear, it's not a good choice for most networks. Don't use Telnet!

#### **D. VNC**

VNC (Virtual Network Computing) is a screen sharing technology that is common to many non-Windows operating systems. If a technician is sharing the screen of a macOS or Linux desktop, they may be using VNC.



#### **More information:**

220-1002, Objective 4.9 - Remote Access Technologies

<https://professormesser.link/1002040901>

**A60.** A user has placed a smartphone on their desk, and they occasionally hear the sound of a camera shutter when the phone is not being used. Which of the following should a technician follow to BEST resolve this issue?

- A.** Put the phone into airplane mode
  - B.** Connect to the corporate network using a VPN connection
  - C.** Run an anti-malware scan on the smartphone
  - D.** Remove any paired Bluetooth devices
- 

**The Answer:** **C.** Run an anti-malware scan on the smartphone

Pictures taken when the phone is not in use would be considered an unauthorized use of the camera. This suspicious activity should be researched further and an anti-malware scan should be used to start testing for any security issues.

**The incorrect answers:**

**A.** Put the phone into airplane mode

Disconnecting all network connections may be part of the troubleshooting process, but simply using airplane mode would not resolve the issue of unauthorized camera use.

**B.** Connect to the corporate network using a VPN connection

Any connection to the corporate office from a remote location should use a VPN (Virtual Private Network) connection, but using this encrypted tunnel would not resolve a smartphone with unauthorized camera use.

**D.** Remove any paired Bluetooth devices

Although some Bluetooth devices can be used to take remove pictures, in this situation the camera was active when the phone was not in use. This almost certainly indicates malware or some other unauthorized process is running on the smartphone.



**More information:**

220-1002, Objective 3.5

Troubleshooting Mobile Device Security

<https://professormesser.link/1002030501>

**A61.** Sam, a user on the research and development team, reports that her computer displays the message “Missing operating system” during boot. A technician runs hardware diagnostics and finds that the RAM, CPU, storage drive, and power supply all pass the tests. The technician then finds that a connected USB flash drive was causing the issue. Which of the following would prevent this issue from occurring in the future?

- A.** Update the BCD
  - B.** Install the latest OS patches
  - C.** Run SFC
  - D.** Modify the BIOS boot order
- 

**The Answer:** **D.** Modify the BIOS boot order

If the BIOS is configured to boot from a USB interface prior to the internal storage drive, then any bootable flash drive would be used as a boot device. In this case, modifying the BIOS boot order would cause the system to boot from an internal drive first before attempting to boot from another device.

**The incorrect answers:**

**A.** Update the BCD

The BCD (Boot Configuration Data) is used by Windows to determine the location of a valid Windows operating system. Updating the BCD would not stop a flash drive from booting prior to the internal storage drive.

**B.** Install the latest OS patches

Patching the operating system would not prevent the USB interface from booting before the internal storage drive.

**C.** Run SFC

System File Checker is a Windows utility that will verify the integrity of the core operating system files. Running the SFC utility will not prevent the system from attempting to boot from a USB-connected drive.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1002030101>

**A62.** Jack, a user, has opened a help desk ticket relating to email messages he's receiving. The messages appear to be replies to a message that Jack did not send. Most of the messages contain information about third-party product promotions and sales information. Which of the following is the MOST likely cause of these messages?

- A. Man-in-the-middle
  - B. Corrupted email database
  - C. Adware
  - D. Hijacked email
- 

**The Answer:** D. Hijacked email

Of the available options, the most likely reason for these unusual email replies is a hijacked email account. An attacker that gains access to an email account can send spam, read messages, and effectively control all emails associated with the account. Common responses to an email hijacking are to change the passwords associated with the account and scan for malware.

**The incorrect answers:**

**A. Man-in-the-middle**

A man-in-the-middle attack would include a third-party that was intercepting and potentially modifying network data. In this situation, there's no evidence that a third-party is intercepting any network communication.

**B. Corrupted email database**

A corrupted email database would cause the user's emails to be unreadable or would cause messages to be missing. Most email platforms will recognize a corrupted database and would not allow the user to access their mailbox.

**C. Adware**

Adware would show advertising and sales messages to the infected user and would not commonly send email messages to other users.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues

<https://professormesser.link/1002030201>

**A63.** In which of the following file types would a system administrator expect to see the command, "cd c:\source"?

- A. .sh
  - B. .vbs
  - C. .py
  - D. .bat
- 

**The Answer: D. .bat**

The .bat file extension refers to the Windows batch files. The "cd" command can refer to many different operating systems, but the reference to the drive letter "c:" is common to the Windows operating system.

**The incorrect answers:**

**A. .sh**

The .sh extension is a shell script. Scripts that run in Linux, Unix, or macOS often use the .sh extension to designate a file as a shell script.

**B. .vbs**

Microsoft Visual Basic Scripting Edition scripts are commonly called VBScript and use the extension .vbs. A VBScript would not use the cd command and drive letters.

**C. .py**

Python scripts often use the .py extension. Python has its own method of managing files and would not use the Windows "cd" command.



**More information:**

220-1002, Objective 4.8 - Scripting

<https://professormesser.link/1002040801>

**A64.** A malware infection has recently been removed from a computer. When starting the operating system, Windows shows errors during the startup process indicating some core operating system files are missing. Which of the following should be used to restore these missing files?

- A. gpupdate
  - B. dism
  - C. sfc
  - D. diskpart
- 

**The Answer: C. sfc**

The sfc (System File Checker) command is used to scan and replace any core operating system files that may be corrupted or missing. It's common to run the sfc utility after removing malware or after a significant operating system issue.

**The incorrect answers:**

**A. gpupdate**

The gpupdate (Group Policy Update) command is used to force a Group Policy update to computers in a Windows Active Directory domain. The gpupdate command would not restore any missing operating system files.

**B. dism**

The dism (Deployment Image Servicing and Management) tool is used to make changes to Windows Imaging Format (WIM) files. This question did not specify that the computer was using a WIM file, so the dism utility would not be the best choice to restore any missing files.

**D. diskpart**

An administrator can manage disk configurations and partitions with the Windows diskpart utility. The diskpart utility is not used to restore or modify files within the Windows operating system.



**More information:**

220-1002, Objective 1.4 - Microsoft Command Line Tools  
<https://professormesser.link/1002010401>

**A65.** A desktop administrator has determined that an employee in the corporate office has been using their computer to share copyrighted materials to others on the Internet. Which of the following should be the best NEXT step?

- A.** Create a firewall rule to block Internet access to this computer
  - B.** Create a hash for each file that was shared
  - C.** Compile a list of licenses for each set of copyrighted materials
  - D.** Retrieve and securely store the computer
- 

**The Answer:** **D.** Retrieve and securely store the computer

When a security incident has occurred, it's important to securely collect and store any evidence. The computer that was used to share copyrighted materials should be collected and stored until the proper authorities can take control of this evidence.

**The incorrect answers:**

**A.** Create a firewall rule to block Internet access to this computer

Creating a firewall rule would stop anyone from accessing the computer, but it wouldn't stop the user from modifying or deleting files and evidence from the PC.

**B.** Create a hash for each file that was shared

Although creating hashes of the files may be part of the evidence gathering process, the immediate need is to impound and protect the data on the system used in this event.

**C.** Compile a list of licenses for each set of copyrighted materials

The determination of copyright is part of the process that will occur later. The more important task will be to collect the evidence and protect its integrity.



**More information:**

220-1002, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1002040601>

**A66.** A system administrator would like to require a specific password complexity for all Active Directory users. Which of the following would be the BEST way to complete this requirement?

- A.** Login script
  - B.** Folder redirection
  - C.** Port security
  - D.** Group Policy
- 

**The Answer:** **D.** Group Policy

Group Policy is the centralized management feature of Active Directory, and allows an administrator to define specific desktop and security policies, including the minimum complexity of passwords.

**The incorrect answers:**

**A.** Login script

A login script is executed after a user has completed the initial login process. The password complexity policy would need to be active prior to the authentication process.

**B.** Folder redirection

Folder redirection allows a Windows administrator to redirect user storage from a local folder to a server share. This allows for the centralized storage of files and the ability to access the files from anywhere on the network.

The folder redirection would not change password complexity policies.

**C.** Port security

Port security is used to prevent unauthorized users from connecting to a switch interface. Port security does not define any parameters for password complexity.



**More information:**

220-1002, Objective 2.2 - Logical Security

<https://professormesser.link/1002020201>

**A67.** A system administrator is creating a series of shared folders that should not be visible when users browse the network for available shared resources. What symbol should be added to the end of a share name to provide this functionality?

- A.** . (period)
  - B.** \$ (dollar sign)
  - C.** ! (exclamation mark / bang)
  - D.** # (hash sign / number sign)
- 

**The Answer:** **B.** \$ (dollar sign)

Windows shares ending with a dollar sign (\$) are hidden and won't be shown in the normal list of available shares. The hidden share can still be accessed if the user knows the name of the share, so this should not be considered a security feature.

**The incorrect answers:**

**A.** . (period)

Ending the Windows share with a period is not supported.

**C.** ! (exclamation mark / bang)

Using the exclamation mark in a share name is not supported.

**D.** # (hash sign / number sign)

The hash sign is not allowed in a share name.



**More information:**

220-1002, Objective 1.8 - Windows Network Technologies

<https://professormesser.link/1002010802>

**A68.** Jack, a user, is having problems with the 802.11 wireless connection on his iOS phone. Although there are names appearing in the network list, his phone does not show any connectivity to a wireless network. Jack has confirmed that airplane mode is not enabled, Bluetooth is on, and VPN is not enabled. Which of the following is the MOST likely reason for this lack of wireless connectivity?

- A. The phone does not include a data plan
  - B. The wireless network is not active
  - C. The Bluetooth connection is conflicting with the Wi-Fi
  - D. The Wi-Fi password is incorrect
  - E. The wireless radio is disabled
- 

**The Answer:** D. The Wi-Fi password is incorrect

Since wireless network names are visible and Jack is not connected to one of the available networks, it's most likely that the authentication process has failed.

**The incorrect answers:**

A. The phone does not include a data plan

The status of a cellular data plan does not have any effect on the connectivity to Wi-Fi networks.

B. The wireless network is not active

Wireless network names are appearing in the network list, so the wireless network is clearly active with multiple networks.

C. The Bluetooth connection is conflicting with the Wi-Fi

Bluetooth frequencies are commonly active on unused portions of the 2.4 GHz spectrum. Bluetooth will not conflict with Wi-Fi communication.

E. The wireless radio is disabled

Since network names appear in the phone's list of available Wi-Fi networks, we can assume that the wireless radio is active.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**A69.** A desktop administrator is upgrading the video adapter in a CAD/CAM workstation. Which of the following should the administrator use during this process?

- A.** Tone generator
  - B.** Anti-static strap
  - C.** Safety goggles
  - D.** Toner vacuum
- 

**The Answer:** **B.** Anti-static strap

Electrostatic discharge (ESD) is always a concern when working with the components inside of a computer. To minimize the potential for static discharge, it's always a good idea to use a static strap and other anti-static mats and bags.

**The incorrect answers:**

**A.** Tone generator

A tone generator is used to locate the two ends of a copper cable. A tone generator would not be used during a video adapter upgrade.

**C.** Safety goggles

Safety goggles may be necessary when toner or excessive dust particles are in the air, but it's not common to need safety goggles when replacing adapter cards.

**D.** Toner vacuum

A toner vacuum would only be necessary if there was a toner spill that needed to be cleaned. A toner vacuum would not be used during an adapter card upgrade.



**More information:**

220-1002, Objective 4.4 - Managing Electrostatic Discharge  
<https://professormesser.link/1002040402>

**A70.** A help desk director would like to identify and track computer systems that have been returned for service or moved from one location to another. Which of the following would be the BEST solution for these requirements?

- A.** Cable labels
  - B.** Asset tags
  - C.** Topology diagrams
  - D.** Login names
- 

**The Answer:** **B.** Asset tags

It's common for equipment to move between users, buildings, or departments. To keep track of this equipment, it's common to attach an internal asset tag to clearly show the equipment is owned by the company and to track the equipment using the internal reference number.

**The incorrect answers:**

**A.** Cable labels

A cable label is commonly used to mark the two ends of a cable. This allows the user to confirm the correct connectors without using a tone generator or cable tester. Cable labels would not be used to track equipment.

**C.** Topology diagrams

One common use of a topology diagram is for the network team to document the traffic flow through the organization's switches, routers, and other infrastructure equipment. A topology diagram would not be used to track other company assets.

**D.** Login names

Login names are not associated with any particular piece of hardware. It would not be useful to track laptops, desktops, and other equipment using login names.



**More information:**

220-1002, Objective 4.1 - Documentation Best Practices

<https://professormesser.link/1002040101>

**A71.** A technician is troubleshooting a computer infected with a virus. The user thought they were opening a spreadsheet, but the file was actually a virus executable. Which of the following Windows options were MOST likely associated with this issue?

- A.** Always show icons, never thumbnails
  - B.** Display the full path in the title bar
  - C.** Always show menus
  - D.** Hide extensions for known file types
- 

**The Answer:** **D.** Hide extensions for known file types

With extensions hidden, it's difficult to know the type of file just based on the filename. A filename named "Monthly Orders" might be a spreadsheet, or it could be an executable containing a virus.

**The incorrect answers:**

**A.** Always show icons, never thumbnails

Showing icons instead of thumbnails can still be a way to hide information. For example, it's relatively easy to create an executable that uses the same icon as a spreadsheet.

**B.** Display the full path in the title bar

The full path in the title bar shows where the file is located on the volume, but it doesn't provide any information about the contents of the file.

**C.** Always show menus

The Windows menus are useful, but the menus themselves don't provide any additional information about the contents of a particular file.



**More information:**

220-1002, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1002010601>

**A72.** A financial management company would like to ensure that mobile users are configured with the highest level of wireless encryption while working in the office. They would also like to include an additional user verification step during the login process. Which of the following would provide this functionality? (Choose TWO)

- A.** RADIUS
  - B.** WPS
  - C.** Multi-factor authentication
  - D.** TKIP
  - E.** TACACS
  - F.** RC4
  - G.** WPA2
- 

**The Answer:** **C.** Multi-factor authentication, and **G.** WPA2

Multi-factor authentication requires the user to login using two different methods, such as a password and a generated token. WPA2 (Wi-Fi Protected Access version 2) enables strong encryption for all wireless communication.

**The incorrect answers:**

**A.** RADIUS

RADIUS (Remote Authentication Dial-in User Service) is an authentication technology, but RADIUS itself does not provide an additional user verification.

**B.** WPS

WPS (Wi-Fi Protected Setup) is a wireless authentication method that is designed to make it easier for devices to connect to a wireless network. WPS itself does not include any additional user verification or encryption methods.

#### **D. TKIP**

TKIP (Temporal Key Integrity Protocol) was used with the initial version of WPA to ensure data integrity and to prevent data tampering.

#### **E. TACACS**

TACACS (Terminal Access Controller Access-Control System) is an authentication protocol. TACACS itself does not provide any additional user verification or network encryption technologies.

#### **F. RC4**

RC4 (Rivest Cipher 4) was used with the first version of WPA to provide data encryption. RC4 does not provide any additional user verification, and vulnerabilities with RC4 have caused it to be replaced with AES (Advanced Encryption Standard) in WPA2.



#### **More information:**

220-1002, Objective 2.3 - Wireless Security

<https://professormesser.link/1002020301>

**A73.** A network consulting firm is creating a proposal to upgrade the Internet firewalls for a large corporation. The proposal includes a description of the project and the network topology changes that would be required to support the upgrade. The proposal also describes the risks involved in the process of making this upgrade. Which of the following should be covered NEXT in the proposal?

- A.** End-user approvals
  - B.** Backout plan
  - C.** Change control application
  - D.** Detailed upgrade plan
- 

**The Answer:** **D.** Detailed upgrade plan

Before working through the remaining change control steps, it's important to have a detailed explanation of the steps that will be required to complete the change. This detailed plan will provide decision-making information to the change control board and provide the information needed to create a backout plan.

**The incorrect answers:**

**A.** End-user approvals

Without a detailed plan, it's difficult to determine who the end users are. Since the end-user approvals are required to continue with the change control process, the detailed plan will need to be created first.

**B.** Backout plan

A backout plan can't be created until you know the specific changes that are planned.

**C.** Change control application

The change control committee will need specific details about the proposed changes so they can understand the scope of what they are approving.



**More information:**

220-1002, Objective 4.2 - Change Management

<https://professormesser.link/1002040201>

**A74.** An organization has been tasked with increasing the minimum password length. A systems administrator has created a policy to require all passwords to be at least ten characters long for all users. When testing this policy in the lab, a laptop computer allowed the creation of eight-character passwords. Which of the following commands should be used to apply this new policy on the laptop?

- A.** net use
  - B.** gpupdate
  - C.** sfc
  - D.** tasklist
- 

**The Answer:** **B.** gpupdate

The gpupdate (Group Policy Update) command forces centralized updates to be activated on target devices. In this example, the policy was created but the laptop computer had not yet received the new configuration.

**The incorrect answers:**

**A. net use**

The net use command assigns Windows shares to local drive letters. The net use command will not process Group Policy changes or modify the password policies on a computer.

**C. sfc**

The sfc (System File Checker) utility will scan protected system files to make sure that the core operating system has integrity. The sfc utility will not have any impact on the use of passwords.

**D. tasklist**

The Windows tasklist command displays a list of currently running processes on a local or remote machine. Running tasklist will not change any policies related to password complexity.



**More information:**

220-1002, Objective 1.4 - Microsoft Command Line Tools  
<https://professormesser.link/1002010401>

**A75.** A technician has been tasked with removing malware on a training room laptop. After updating the anti-virus software and removing the malware, the technician creates a backup of the system. After the training class ends, the technician is notified that the malware has returned.

Which of the following steps was missed and caused the system to be infected again?

- A. Boot to a pre-installation environment
  - B. Identify malware symptoms
  - C. Disable System Restore before removal
  - D. Update to the latest BIOS version
- 

**The Answer:** C. Disable System Restore before removal

Malware does not like to be removed from a system, so it does everything it can to stick around. When the malware infects the running operating system, it also infects all of the previous restore points as well. If the restore points aren't removed with the malware, then going back in time to a previous restore point will reinfect the system.

**The incorrect answers:**

**A. Boot to a pre-installation environment**

A pre-installation environment is often required during the remediation phase to assist with the malware removal. The use of a pre-installation environment does not commonly have any effect on future reinfections.

**B. Identify malware symptoms**

Since malware was previously removed from this system, we can assume that the malware was originally identified.

**D. Update to the latest BIOS version**

Updating the BIOS isn't commonly considered part of the malware removal process, and using an older BIOS version doesn't generally cause a device to be more susceptible to malware infections.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**A76.** A data center manager requires each server to maintain at least fifteen minutes of uptime during a power failure. Which of these would be the BEST choice for this requirement?

- A.** Cloud-based storage
  - B.** UPS
  - C.** Redundant power supplies
  - D.** Surge suppressor
- 

**The Answer: B. UPS**

A UPS (Uninterruptible Power Supply) provides short-term backup power if a power outage or low-voltage situation was to occur.

**The incorrect answers:**

**A. Cloud-based storage**

The use of cloud-based storage does not provide any server uptime if a power outage occurs.

**C. Redundant power supplies**

Some servers might use redundant power supplies to maintain uptime if one of the power supplies was to fail. If there's a power outage, then none of the power supplies will be working properly.

**D. Surge suppressor**

A surge suppressor will protect a computer from spikes and noise, but it won't provide any uptime if the primary power source was to fail.



**More information:**

220-1002, Objective 4.3 - Disaster Recovery

<https://professormesser.link/1002040301>

**A77.** A financial corporation is deploying tablets to their salespeople in the field. The company would like to ensure that the data on the tablets would remain private if the devices were ever stolen or lost. Which of the following would be the BEST way to meet this requirement?

- A.** Use full device encryption
  - B.** Require multi-factor authentication
  - C.** Install a locator application
  - D.** Use a firewall app
- 

**The Answer:** **A.** Use full device encryption

Full device encryption ensures that all of the information on the tablet cannot be viewed by anyone outside of the company. If the tablet were lost or stolen, all of the data on the device would remain private.

**The incorrect answers:**

**B.** Require multi-factor authentication

Multi-factor authentication adds additional login requirements, but that doesn't necessarily protect the data already stored on the tablet. If someone was to bypass the multi-factor authentication process, the data would still be at risk.

**C.** Install a locator application

A locator application would allow system administrators to view the location of the tablet, but it wouldn't provide any additional security for the data on the device.

**D.** Use a firewall app

A firewall app would keep unauthorized users from accessing the tablet over the network, but it would not provide any protection for the data that is already stored on the tablet.



#### More information:

220-1002, Objective 2.8 - Securing Mobile Devices

<https://professormesser.link/1002020801>

**A78.** A system administrator is adding an additional drive to a server and extending the size of an existing volume. Which of the following utilities would provide a graphical summary of the existing storage configuration?

- A.** Disk Management
  - B.** Performance Monitor
  - C.** Event Viewer
  - D.** Task Scheduler
  - E.** Device Manager
- 

**The Answer:** **A.** Disk Management

The Disk Management utility provides a graphical overview of the current disk configuration, status, free space, and other important metrics.

**The incorrect answers:**

**B.** Performance Monitor

The Performance Monitor provides a historical summary of system performance and resource utilization.

**C.** Event Viewer

The Event Viewer maintains all of the application and system logs for Windows devices.

**D.** Task Scheduler

The Windows Task Scheduler can automate scripts and applications to run at predetermined times.

**E.** Device Manager

The Windows Device Manager is the management interface to the device drivers and other hardware components. The storage drives are not managed through the Device Manager



**More information:**

220-1002, Objective 1.5 - Disk Management

<https://professormesser.link/1002010505>

**A79.** While using a laptop during presentations, a company vice president has found that her system randomly locks up. While the problem is occurring, the screen continues to display the last presentation slide but none of the mouse or keyboard buttons will work. To regain control, the vice president must power down and reboot her computer. Which of the following would be the BEST option for troubleshooting this issue?

- A. Examine the Task Manager
  - B. Install an anti-malware utility
  - C. Run the presentation software in Safe Mode
  - D. Check the Event Viewer
- 

**The Answer:** D. Check the Event Viewer

Random lock-ups are always a mystery. The Windows Event viewer can provide important information about events that may have occurred just prior to the issue and afterwards.

**The incorrect answers:**

**A.** Examine the Task Manager

The Windows Task Manager will display a list of the currently running processes, but it won't provide any troubleshooting information about application crashes or problems.

**B.** Install an anti-malware utility

Although the issue could be related to almost anything, it's a bit too early in the troubleshooting process to start making changes and installing additional software.

**C.** Run the presentation software in Safe Mode

Without knowing more about the issue, running the system in Safe Mode would not guarantee any particular benefit.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues

<https://professormesser.link/1002030201>

**A80.** A system administrator has booted a computer using PXE. Which of the following would be the MOST likely reason for this task?

- A.** Monthly OS patch install
  - B.** OS installation from a network drive
  - C.** Boot to Safe Mode
  - D.** Control the computer remotely
- 

**The Answer:** **B.** OS installation from a network drive

PXE (Preboot eXecution Environment), or "Pixie," is a method of booting a computer from an image file located on a network server. One common use of PXE boots are to install an operating system across many systems at the same time.

**The incorrect answers:**

**A.** Monthly OS patch install

It's not necessary to boot from a network drive to install the monthly Microsoft operating system patches.

**C.** Boot to Safe Mode

Booting into Safe Mode can be managed on a local computer without the requirement of booting across the network using PXE.

**D.** Control the computer remotely



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**A81.** A user has opened a help desk ticket for application slowdowns and unwanted pop-up windows. A technician updates the anti-virus software, scans, and removes the malware. The technician then schedules future scans and creates a new restore point. Which of the following should be the NEXT step in the removal process?

- A.** Disable System Restore
  - B.** Update the anti-virus signatures
  - C.** Quarantine the system
  - D.** Educate the end user
- 

**The Answer:** **D.** Educate the end user

After the malware has been removed and the system is protected from future infections, it's important to educate the end user on how they could prevent additional problems and when they should contact their support team for additional help.

**The incorrect answers:**

**A.** Disable System Restore

The process of disabling System Restore to remove all of the existing restore points is one of the first steps in the malware removal process and should occur prior to the remediation phase.

**B.** Update the anti-virus signatures

The time to update the anti-virus signatures would be in the initial remediation phase prior to scanning and removing the malware.

**C.** Quarantine the system

A system should be separated from the rest of the systems as soon as malware is suspected. The system would not need to be quarantined after the malware has been successfully removed.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**A82.** A technician is setting up some new computers on an industrial manufacturing floor that cuts wood boards for cabinets. Which of the following would be the MOST important for this setup process?

- A.** ESD mat
  - B.** UPS
  - C.** Anti-static bag
  - D.** Air filter mask
- 

**The Answer:** **D.** Air filter mask

When working in an industrial area with particles in the air, it's important to protect your face and lungs by using a mask that will filter out the contaminants.

**The incorrect answers:**

**A. ESD mat**

An ESD (Electrostatic Discharge) mat is used when working with individual computer components to protect them from damage. This question references the setup of computers, and there's no mention of working inside of the systems or with individual components.

**B. UPS**

A UPS (Uninterruptible Power Supply) is used to maintain a backup power source when the primary power is unavailable. There's no requirement in this question that would need a UPS during the computer setup process, and it's more important to be protected while installing the new computers.

**C. Anti-static bag**

An anti-static bag is used to protect computer components when they are outside of the computer or during transportation. An anti-static bag is not needed during the computer setup process.



**More information:**

220-1002, Objective 4.4 - Safety Procedures

<https://professormesser.link/1002040401>

**A83.** Sam, a user in the accounting department, has opened a help desk ticket due to problems accessing the website of the company's payroll service provider. The help desk technician finds that other users in the accounting department are able to successfully access the website. While testing other website connections on Sam's computer, the technician finds that many pop-up windows are displayed. Which of the following would be the BEST way for the technician to resolve this issue?

- A. Uninstall the browser and reinstall with a different version
  - B. Restore the workstation from a known good backup
  - C. Start in Safe Mode and connect to the payroll website
  - D. Modify the browser's proxy settings
- 

**The Answer:** B. Restore the workstation from a known good backup  
The help desk technician found the problem only appeared on Sam's workstation and the problems appeared to indicate a malware infection. Given the available answers, the only one that would provide a resolution is to restore the system from a known good backup.

**The incorrect answers:**

A. Uninstall the browser and reinstall with a different version

If a system is infected with malware, uninstalling the browser and reinstalling another version will not resolve the issue. To guarantee removal of the malware, the entire system must be deleted and reinstalled.

C. Start in Safe Mode and connect to the payroll website

Safe Mode does not prevent malware from running, and it's unlikely that Safe Mode would provide access to the third-party website.

D. Modify the browser's proxy settings

There's no evidence from the testing that the connectivity issue is related to an incorrect proxy setting. In this example, the large number of pop-up windows appears to indicate a malware infection.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues  
<https://professormesser.link/1002030201>

**A84.** A business partner in a different country needs to access an internal company server during the very early morning hours. The internal firewall will limit the partner's access to this single server. Which of these would be the MOST important security task to perform on this server?

- A.** Install the latest OS patches
  - B.** Remove the server from the Active Directory domain
  - C.** Use only 64-bit applications
  - D.** Run a weekly anti-virus scan
- 

**The Answer:** **A.** Install the latest OS patches

This system will be used during non-working hours from a location that is not part of your organization, so keeping the operating system secure will be important. Maintaining an aggressive patching schedule will ensure that any known vulnerabilities are always removed before they could possibly be exploited.

**The incorrect answers:**

**B.** Remove the server from the Active Directory domain

An Active Directory domain allows a domain administrator to centrally manage security policies and to provide ongoing monitoring of a device. The server would be less secure if it were removed from the AD domain.

**C.** Use only 64-bit applications

There's no enhanced security with 64-bit applications, so ensuring the use of those applications wouldn't provide any significant security advantages.

**D.** Run a weekly anti-virus scan

The concern with this server is that it will be accessed by unknown third-parties from the partner's network. Running an anti-virus scan every week would not provide any significant security benefit, and would probably be delivered too late to be of use.



#### More information:

220-1002, Objective 2.7 - Workstation Security Best Practices

<https://professormesser.link/1002020701>

**A85.** A Linux administrator has been asked to upgrade the web server software on a device. Which of the following would provide the administrator with the appropriate rights and permissions for this upgrade?

- A.** chmod
  - B.** apt-get
  - C.** ifconfig
  - D.** sudo
- 

**The Answer:** **D.** sudo

The sudo (superuser do) command will execute a command as the superuser or any other user on the system. When performing administrative tasks such as upgrading software, it's often necessary to use elevated rights and permissions.

**The incorrect answers:**

**A.** chmod

The chmod (change mode) command will modify the read, write, and execution permissions for a file system object. The mode of a file or folder would not commonly need to be modified during an upgrade.

**B.** apt-get

The apt-get (Advanced Packaging Tool) command is used to manage application packages and software upgrades. The apt-get command does not provide any additional rights and permissions, however.

**C.** ifconfig

The ifconfig (Interface Configuration) command displays or configures a network interface and IP address configuration. No rights or permissions are provided through the ifconfig command.



**More information:**

220-1002, Objective 1.9 - Basic Linux Commands  
<https://professormesser.link/1002010906>

**A86.** A system administrator has installed a new video driver on a laptop computer, but the icons and text on the screen are larger than the previous driver version. Which of the following should be modified to resolve this problem?

- A.** Resolution
  - B.** Color depth
  - C.** Refresh rate
  - D.** Video memory
- 

**The Answer:** **A.** Resolution

The display resolution is the number of vertical and horizontal pixels on the screen. As the screen resolution is lowered, the items on the screen will appear larger.

**The incorrect answers:**

**B.** Color depth

The color depth determines how many colors can be represented on the display. Modifying the color depth will not change the relative sizes of text or icons on the display.

**C.** Refresh rate

The refresh rate refers to the number of updates that the display receives each second. Modifying the refresh rate will not change the relative size of items on the screen.

**D.** Video memory

Most video adapters will include memory that is used by the adapter card to process the video used by the display. Using an adapter with a different memory configuration will not change the size of items on the screen.



**More information:**

220-1002, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1002010601>

**A87.** A network administrator is configuring a wireless network at a small office. The administrator would like to allow wireless access for all computers but exclude a single kiosk in the lobby. Which of the following configuration settings would meet this requirement?

- A. SSID suppression
  - B. Content filtering
  - C. Static IP addressing
  - D. WPS
  - E. MAC filtering
- 

**The Answer:** E. MAC filtering

MAC (Media Access Control) address filtering can be configured to allow or deny access to the network based on the hardware address of the wireless network adapter. Given the available options, MAC filtering would be the only way to provide this type of device exclusion.

**The incorrect answers:**

**A. SSID suppression**

The SSID (Service Set Identifier) is the name of the wireless network, and most access points allow the administrator to control the broadcasting of the network name. This option would not display the name on a list of available wireless networks, but a device could connect to the network if the name was already known.

**B. Content filtering**

Content filtering refers to the control of information inside of an existing data flow. This commonly controls based on the URLs (Uniform Resource Locators) associated with websites, allowing the administrator to allow or deny access to certain categories of online content. This functionality would not be used to limit wireless network access for a single device.

### C. Static IP addressing

Static IP addressing would require the administrator to manually assign IP addresses to all of the devices on the network, but this manual assignment is not a security feature and would not necessarily restrict access to the network from any device.

### D. WPS

WPS (Wi-Fi Protected Setup) is a configuration option on a wireless access point that is designed to make it easier for other devices to connect to the network. The use of WPS does not provide a way to limit or restrict wireless network access if a device already has the proper credentials.



#### More information:

220-1002, Objective 2.10 - Securing a SOHO Network

<https://professormesser.link/1002021001>

**A88.** After booting, a laptop computer is showing a black screen instead of the normal Windows login prompt. The logs from the update server show drivers on the laptop were automatically updated overnight. Which of the following would be the BEST way to resolve this issue?

- A. Reinstall the operating system
  - B. Update the BCD
  - C. Start in VGA mode and roll back the driver
  - D. Upgrade the BIOS
- 

**The Answer:** C. Start in VGA mode and roll back the driver

If a video driver has problems, it becomes difficult to troubleshoot without any video output. In these cases, it's useful to start in the generic VGA mode to regain some use of the operating system. Using System Restore to roll back the driver will restore the previous video driver and configuration.

**The incorrect answers:**

**A.** Reinstall the operating system

Reinstalling the operating system might also install a new video driver and resolve the issue, but it would certainly modify many operating system files and potentially remove user data and configurations from the system.

**B.** Update the BCD

The BCD (Boot Configuration Data) is the Windows boot manager that launches the operating system. Modifying BCD configurations would not modify the video driver configurations in an operating system.

**D.** Upgrade the BIOS

The BIOS does not contain any video drivers for the operating system, and upgrading the BIOS would not resolve this issue.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Solutions  
<https://professormesser.link/1002030102>

**A89.** A security administrator has received an alert that a user's workstation in the shipping department has attempted to communicate to a command and control server for a well-known botnet. The logs on the workstation show that the user manually installed a new Internet browser the previous day. Which of the following would be the BEST next step for troubleshooting this issue?

- A.** Uninstall the new browser
  - B.** Backup the user's documents
  - C.** Roll back to a previous restore point
  - D.** Disable the user's account
- 

**The Answer:** **D.** Disable the user's account

The first step after identifying a malware infection is to quarantine the system. This would include removing the system from the network and preventing the user's account from accessing other network resources.

**The incorrect answers:**

**A.** Uninstall the new browser

Once the new browser was installed, the malware undoubtedly made significant changes to the user's operating system. Uninstalling the browser would not remove the existing malware infection.

**B.** Backup the user's documents

Although it will be important to preserve as much of the data as possible, performing a backup of the user's documents would not be the best next step given the available options.

**C.** Roll back to a previous restore point

If the system is infected with malware, then it's very likely that the previous restore points have also been infected. Rolling back to a previous restore point will most likely not remove the malware.



**More information:**

220-1002, Objective 2.7 - Workstation Security Best Practices  
<https://professormesser.link/1002020701>

**A90.** A technician is installing a new wireless network in a small remote office. Which of the following should the technician choose to provide the highest level of security on the network?

- A.** WPA2
  - B.** MAC filtering
  - C.** Static IP addressing
  - D.** SSID suppression
- 

**The Answer:** **A.** WPA2

WPA2 (Wi-Fi Protected Access 2) encryption is used to protect the data transmitted over the wireless network. WPA2 or similar encryption would be considered to be the highest level of data protection on a wireless network.

**The incorrect answers:**

**B.** MAC filtering

MAC (Media Access Control) filtering is used to allow or deny access to the network based on the hardware address of the wireless adapter. However, MAC filtering can be easily circumvented and is not considered a security feature.

**C.** Static IP addressing

Static IP address would require the network administrator to manually assign IP addresses to the network devices. Static IP addressing does not provide any security features.

**D.** SSID suppression

SSID (Service Set Identifier) suppression will prevent the name of the wireless network from appearing in lists of available networks. SSID suppression does not prevent someone from connecting to the network if they already know the name, and it's not considered a security feature



**More information:**

220-1002, Objective 2.10 - Securing a SOHO Network

<https://professormesser.link/1002021001>

# Practice Exam B

## Performance-Based Questions

**B1.** Match the Windows utility to the function.

Some functions will not have a match.

### Commands:

### Descriptions:

Services	View the long-term CPU utilization of a server
Performance Monitor	Create a database link to an external server
Device Manager	Disable a background process
Event Viewer	Schedule a batch file to run at 3 AM
	Update Windows system files
	View the version number of a device driver
	View the logs associated with an application

- B2.** A network administrator is troubleshooting an intermittent Internet link outage to a server at 8.8.8.8. The administrator believes that the outage is occurring on one of the WAN connections between locations. Use a Windows network utility that can identify the router that is closest to the outage.



Command Prompt  
(c) 2019 Microsoft Corporation. All rights reserved.  
C:\Users\james>

- 
- B3.** Match the scripting language with the most common use.  
Some uses will not have a match.

**Scripting Language:**

**Use:**

VBScript

Disable an Active Directory account

JavaScript

Retrieve statistics from a network device

Python

Import data into an Excel spreadsheet

Batch file

Add animation to a website login screen

Compare files on a Windows workstation

Move log files on a Linux server

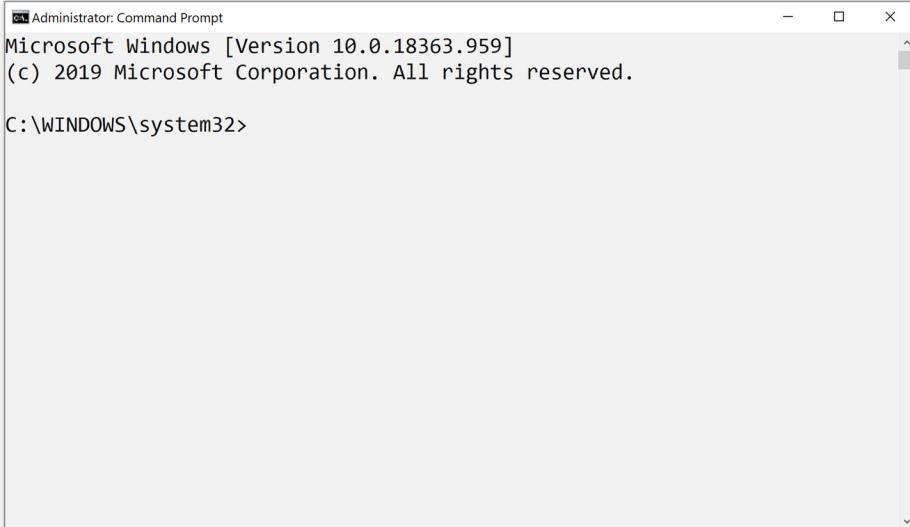
**B4.** Select the Windows 10 Editions that include the following features.

Some features will be included in multiple Windows 10 Editions:

Domain Membership	Home	Pro	Enterprise
AppLocker	Home	Pro	Enterprise
BitLocker	Home	Pro	Enterprise
BranchCache	Home	Pro	Enterprise
Hyper-V	Home	Pro	Enterprise

---

**B5.** A system administrator is concerned that the local Windows file system may contain logical file system errors. Scan and repair any potential file system errors from the Windows command line.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

---



# Practice Exam B

## Multiple Choice Questions

- B6.** A technician is delivering a new laptop to a user and moving the older laptop to a different user. Which of the following would allow the existing hard drive to be used but prevent recovery of any of the previous user's data?
- A. Regular format
  - B. Run a defragmentation
  - C. Connect the laptop to the Windows Domain
  - D. Delete the \Users folder
- Quick  
Answer: **161**
- B7.** A desktop technician is replacing all of the CRT displays on a manufacturing line and replacing them with LCD displays. Which of the following would be the BEST way to dispose of the old monitors?
- A. Take to a hazardous waste facility
  - B. Return to the manufacturer
  - C. Separate the parts and dispose of normally
  - D. Contract with an incineration company
- The Details: **170**
- B8.** A user needs to modify a spreadsheet for an upcoming meeting. The spreadsheet is currently stored on a remote computer in a shared drive. The user would like to access the shared drive as a drive letter inside of Windows File Explorer. Which of the following command line options would provide this functionality?
- A. tasklist
  - B. net use
  - C. diskpart
  - D. netstat
- Quick  
Answer: **161**
- The Details: **171**
- The Details: **172**

**B9.** A macOS server administrator needs a backup system that will allow the recovery of data from any point in the last thirty days. Which of the following should be used for this requirement?

- A.** Backup and Restore
- B.** Boot Camp
- C.** Spaces
- D.** Time Machine

Quick  
Answer: **161**

The Details: **173**

**B10.** Why would a technician use an ESD strap?

- A.** Protects electronic parts from extreme heat
- B.** Keeps electronic parts dry and free from moisture
- C.** Prevents damage from static electricity
- D.** Protects computer parts from dust

Quick  
Answer: **161**

The Details: **174**

**B11.** A desktop administrator is upgrading an older computer to support the 64-bit version of Windows 10 Pro. The computer currently has:

1 GHz CPU  
1 GB of RAM  
50 GB of free storage space  
1024 x 768 video resolution

Which of the following should be upgraded to support the Windows 10 installation?

- A.** CPU
- B.** RAM
- C.** Storage space
- D.** Video resolution

Quick  
Answer: **161**

The Details: **175**

**B12.** Jack, a technician, is scheduled to replace a faulty motherboard today, but the motherboard delivery has been delayed and will not arrive until tomorrow. The new motherboard will repair a laptop used by a company executive. Which of the following would be the BEST way to handle these events?

- A. Move the installation to the next business day
- B. Schedule another repair into today's newly opened time slot
- C. Ask the delivery company for a refund on the shipping charges
- D. Contact the end user and inform them of the shipping issue

Quick  
Answer: **161**

The Details: **176**

**B13.** A system administrator has been tasked with locating all of the log files contained within an application folder. The folder currently contains over a thousand files, and only a portion of them have a .log extension. Which of these Windows commands would be the BEST way to find these files?

- A. sfc
- B. ls
- C. tasklist
- D. dir

Quick  
Answer: **161**

The Details: **177**

**B14.** A user runs a corporate app on their smartphone that downloads a database each time the app is started. This download process normally takes a few seconds, but today the download is taking minutes to complete. Which of the following should a technician follow as the best NEXT troubleshooting step?

- A. Disable Bluetooth
- B. Run a network speed check
- C. Evaluate the app with an app scanner
- D. Check the cloud storage resource usage

Quick  
Answer: **161**

The Details: **178**

**B15.** A system administrator is analyzing a problem with a USB flash drive on a Windows 10 computer. When the flash drive is inserted, the CPU utilization increases to 100%. The administrator would like to disable one of the computer's USB controllers for troubleshooting. Which of the following would provide this functionality?

- A. Services
- B. Performance Monitor
- C. Event Viewer
- D. Device Manager

Quick  
Answer: **161**

The Details: **179**

**B16.** A user is reporting that some apps launched on their mobile phone will show an error message and then disappear without starting. This problem occurs with a group of apps that are normally used during the work day. Which of the following tasks would be the FIRST step for troubleshooting this issue?

- A. Install the previous version of the apps
- B. Connect the phone to a power source
- C. Power cycle the phone
- D. Disable the GPS radio

Quick  
Answer: **161**

The Details: **180**

**B17.** A technician has been asked to power down and store a server that has been exploited by an external attacker. The legal department will be performing tests and gathering information from this server. Which of the following would be MOST important to ensure the integrity of the server data?

- A. Report the server location to the proper channels
- B. Compile all support tickets associated with the server
- C. Maintain a chain of custody
- D. Take photos of the server in the storage room

Quick  
Answer: **161**

The Details: **181**

**B18.** Jack, a user, has opened a help desk ticket to remove malware from his laptop. A previous removal occurred two weeks earlier with a similar malware infection. Which of the following was missed during the first malware removal?

- A.** Restart the computer
- B.** Educate the end-user
- C.** Enable System Protection
- D.** Quarantine infected systems

Quick  
Answer: **161**

The Details: **182**

**B19.** Which of the following features would be found in Windows 10 Enterprise but not in Windows 10 Pro? (Choose TWO)

- A.** Domain membership
- B.** BitLocker
- C.** BranchCache
- D.** Hyper-V
- E.** Remote Desktop host
- F.** AppLocker

Quick  
Answer: **161**

The Details: **183**

**B20.** A medical research company is using laptop computers when visiting testing centers. The IT security team is concerned about a private medical data breach if a laptop is lost or stolen. Which of the following would be the BEST way to manage this issue?

- A.** BIOS password
- B.** Authenticator app
- C.** Full disk encryption
- D.** Biometric authentication
- E.** Cable lock

Quick  
Answer: **161**

The Details: **184**

**B21.** A user would like to encrypt a small group of files in a shared folder without affecting other files on the drive. Which of the following would be the BEST way to accomplish this?

- A.** EFS
- B.** Save the files "as Administrator"
- C.** BitLocker
- D.** Save the files with a dollar sign at the end of the filename

Quick  
Answer: **161**

The Details: **185**

**B22.** A mobile user has transitioned to using apps on their smartphone for all business tasks. To ensure that no data will be lost, the smartphone will need to have multiple backups each day. The user travels most of the time and rarely visits the home office. Which of the following would be the best way to provide these backups?

- A.** Connect an external USB drive
- B.** Use incremental backups each night
- C.** Connect the smartphone to a laptop
- D.** Use a cloud backup service

Quick  
Answer: **161**

The Details: **186**

**B23.** A desktop administrator is moving an SSD from one laptop to another. Which of the following should be used to protect the SSD during the move?

- A.** Padded envelope
- B.** Anti-static bag
- C.** Box with foam filler
- D.** Cloth wrap

Quick  
Answer: **161**

The Details: **187**

**B24.** A user is performing a series of Google searches, but the results pages are displaying links and advertisements from a different website. This issue occurs each time a Google search is performed. The same Google search on a different computer results in a normal Google results page. Which of the following would resolve this issue?

- A.** Run the search from Safe Mode
- B.** Install the latest operating system patches
- C.** Run a malware removal utility
- D.** Login as a different user

Quick  
Answer: **161**

The Details: **188**

**B25.** Jack, a user in the accounting department, is having an issue with his smartphone reaching websites and retrieving mail when working from home. Inside the office, the phone appears to work normally. Which of the following would be the best NEXT step for troubleshooting this issue?

- A. Verify the network configuration at home
- B. Install the latest operating system updates
- C. Connect the phone to power when working at home
- D. Restart the smartphone after arriving at home

Quick  
Answer: **161**

The Details: **189**

**B26.** A security administrator has been asked to reinstall Windows on a web server diagnosed with a rootkit infection. Which of the following installation methods would be the BEST choice for this server?

- A. In-place upgrade
- B. Multiboot
- C. Clean install
- D. Repair installation

Quick  
Answer: **161**

The Details: **190**

**B27.** A local coffee shop has a public wireless network for customers and a private wireless network for company devices. The shop owner wants to be sure that customers can never connect to the company network. Which of the following should be configured on this network?

- A. Enable WPS on the customer network
- B. Configure WPA2 on the company network
- C. Require static IP addresses on the customer network
- D. Assign MAC filters to the company network
- E. Use a firewall between the customer and corporate network

Quick  
Answer: **161**

The Details: **191**

**B28.** A user in the shipping department has logged into the Windows domain. However, the desktop does not show the user's normal wallpaper and all of the user's spreadsheets and documents in the "My Documents" folder are missing. Which of these would be the BEST way to restore the user's normal work environment?

- A.** Rename the user's folder and delete their profile in the registry
- B.** Boot into Safe Mode and disable all startup applications
- C.** Add the user to the Administrator group
- D.** Update to the latest operating system version

Quick  
Answer: **161**

The Details: **192**

**B29.** A company's shipping department maintains ten different computers to print shipping labels and track outgoing shipments. All of the systems are displaying an error when they try to access a third-party shipping management website over a secure connection. Which of the following would be the MOST likely reason for this issue?

- A.** The computers have not been updated with the latest OS patches
- B.** The website certificate has expired
- C.** The local computer storage drives are not encrypted
- D.** The systems are infected with malware

Quick  
Answer: **161**

The Details: **193**

**B30.** A manufacturing company performs a third-party audit of their accounting records each year. The auditors use laptops provided by the company to access internal resources. When the audit is complete, the auditors should be prevented from logging on until the following audit process begins. Which of the following would be the BEST way to accomplish this?

- A.** Uninstall the audit software
- B.** Disable the accounts between audits
- C.** Remove the auditor accounts from all Windows groups
- D.** Require two-factor authentication for the auditor accounts

Quick  
Answer: **161**

The Details: **194**

**B31.** A manufacturing company is donating some older computers to a local charity. Which of the following should be done to ensure that the existing hard drives could still be used but none of the existing data would be recoverable?

- A.** Degaussing
- B.** Regular format
- C.** Shredder
- D.** Quick format

Quick  
Answer: **161**

The Details: **195**

**B32.** A user is working on a video editing workstation that often performs an overnight rendering process. On some mornings, the user is presented with a login screen instead of the rendering completion page. A technician finds that the site occasionally loses power overnight. Which of the following should be used to avoid these issues with the video editing workstation?

- A.** Use a surge suppressor
- B.** Save the rendered file to an external storage drive
- C.** Create a separate partition for user documents
- D.** Install a UPS

Quick  
Answer: **161**

The Details: **196**

**B33.** A desktop administrator is troubleshooting an older computer that has been slowing down as more applications and files are stored on the hard drive. Which of the following commands would be the BEST choice for increasing the performance of this computer?

- A.** defrag
- B.** format
- C.** sfc
- D.** mstsc
- E.** dxdiag

Quick  
Answer: **161**

The Details: **197**

**B34.** A user in the accounting department has opened a help desk ticket regarding their email messages. There are reports of receiving unusual emails from the user, but the user has not sent any of these messages. A check of the unusual emails shows that they have been sent from the company's internal email server. Which of the following would be the best NEXT step in this troubleshooting process?

- A.** Update the OS patches on the email server
- B.** Run an anti-malware utility on the systems that received the emails
- C.** Reimage the user's computer
- D.** Change the user's email password

Quick  
Answer: **161**

The Details: **198**

**B35.** A system administrator has inadvertently installed a Trojan horse that has deleted a number of files across many Windows file shares. The Trojan also had access to user documents and login credentials and transmitted numerous documents to an off-site file storage system. Which of the following would limit the scope of future exploits?

- A.** Require multi-factor authentication
- B.** Disable all guest accounts
- C.** Modify the default permissions
- D.** Configure full disk encryption
- E.** Require complex passwords
- F.** Require a screensaver password

Quick  
Answer: **161**

The Details: **199**

**B36.** A technician has created an image that can be used across all of the computers in a training room. Which of the following would be the best way to deploy these images?

- A.** Clean install
- B.** PXE
- C.** Repair installation
- D.** Multiboot

Quick  
Answer: **161**

The Details: **201**

**B37.** Which of the following Windows Share permissions has the priority when assigning access on a mapped drive?

- A. Allow
- B. Full control
- C. List folder contents
- D. Deny

Quick  
Answer: **161**

The Details: **202**

**B38.** A data center manager would like to ensure that a power fault on a server would not be harmful to employees. Which of the following would be the BEST choice for this requirement?

- A. Electrical ground
- B. UPS
- C. Air filter mask
- D. ESD mat

Quick  
Answer: **161**

The Details: **203**

**B39.** A user in the shipping department has received a call from someone claiming to be from the IT Help Desk. The caller asks the user to disclose their location, employee ID, and login credentials. Which of the following would describe this situation?

- A. Denial of service
- B. Social engineering
- C. Brute force
- D. Man-in-the-middle

Quick  
Answer: **161**

The Details: **204**

**B40.** A desktop administrator has just removed malware from a user's desktop computer and has configured the system to automatically update anti-virus signatures and perform a scan each night. Which of the following should be the NEXT step in the removal process?

- A. Enable System Protection
- B. Educate the end-user
- C. Quarantine the computer
- D. Boot to Safe Mode

Quick  
Answer: **161**

The Details: **205**

**B41.** A security administrator is installing a new VPN connection for remote users. The administrator would like all users to authenticate with their usual Windows Active Directory credentials. Which of the following technologies would provide this functionality?

- A. RADIUS
- B. WPA2
- C. TKIP
- D. WEP

Quick  
Answer: **161**

The Details: **206**

**B42.** Which of the following partition types limit a Windows installation to a maximum partition size of 2 TB?

- A. FAT32
- B. GPT
- C. NTFS
- D. MBR

Quick  
Answer: **161**

The Details: **207**

**B43.** A system administrator has just completed an update of fifty servers to the latest version of an application, and the updated software has been working as expected for the last three days. Which of the following change management steps should be followed NEXT?

- A. Create a backout plan
- B. Determine the scope of the changes
- C. Document the changes
- D. Determine the risk for the upgrade process

Quick  
Answer: **161**

The Details: **208**

**B44.** A help desk technician has been tasked with rebuilding an email server that recently crashed. Which of the following would be the BEST source for this information?

- A. Compliance report
- B. Acceptable use policies
- C. Network topology map
- D. Knowledge base

Quick  
Answer: **161**

The Details: **209**

**B45.** A server administrator is installing a 4 TB drive in a database server and would like to use the entire free space as a single partition. Which of the following technologies should be used with this drive?

- A.** FAT32
- B.** MBR
- C.** NFS
- D.** GPT

Quick  
Answer: **161**

The Details: **210**

**B46.** A user has called the help desk to get assistance with random blue screens on their Windows 10 laptop. The technician finds that CPU utilization is constantly high, and many network sites are unavailable or only load half of the site content. The user mentions that some random pop-up messages have appeared on the desktop during the workday. Which of the following would be the MOST likely reason for these issues?

- A.** Storage drive is failing
- B.** Network proxy settings are incorrect
- C.** Operating system needs to be updated
- D.** Laptop has a malware infection
- E.** Video subsystem is faulty

Quick  
Answer: **161**

The Details: **211**

**B47.** A technician is troubleshooting an issue with an iOS tablet randomly restarting during normal use. A check of the device shows there have been no significant application updates and the operating system was upgraded to a new version three days ago. The user states the tablet was working normally last week. Which of the following would be the MOST likely reason for these random reboots?

- A.** Faulty OS upgrade
- B.** Invalid device certificate
- C.** Malware infection
- D.** Faulty battery
- E.** Incorrect network settings

Quick  
Answer: **161**

The Details: **212**

- B48.** A system administrator needs to modify a file in the \Windows\Installer directory, but the folder doesn't appear in the file list. Which of these options would help the system administrator with this task?
- A.** Safe Mode
  - B.** File Explorer Options
  - C.** User Accounts
  - D.** Internet Options
- B49.** A Linux administrator is modifying a log file and needs to rename the file. Which of the following should be used to make this change?
- A.** rm
  - B.** mv
  - C.** mkdir
  - D.** pwd
- B50.** A desktop administrator is troubleshooting poor performance on a user's laptop computer. The system takes an excessive amount of time during the boot process, and pop up messages appear while using the word processor and spreadsheet applications. Which of the following steps should the technician do NEXT?
- A.** Educate the end-user
  - B.** Schedule periodic anti-virus scans
  - C.** Enable System Protection
  - D.** Disconnect the laptop from the network
- B51.** Jack, an executive, has a laptop that runs very slowly after login and continues running slowly throughout the day. Jack has complained that certain applications cannot be started and others will randomly crash. A check of the laptop shows that the memory utilization is very close to 100%. Which of the following would provide a short-term fix for this issue?
- A.** Disable startup items
  - B.** Update to the latest OS patches
  - C.** Defragment the hard drive
  - D.** Reboot the computer

Quick  
Answer: **161**

The Details: **213**

Quick  
Answer: **161**

The Details: **214**

Quick  
Answer: **161**

The Details: **215**

Quick  
Answer: **161**

The Details: **216**

**B52.** A help desk technician needs to view and control the desktop of a Windows computer at a remote location. Which of the following would be the BEST choice for this task?

- A.** Telnet
- B.** VNC
- C.** SSH
- D.** RDP

Quick  
Answer: **161**

The Details: **217**

**B53.** The storage drive in a user's laptop has recently failed, and a temporary laptop was assigned to the user during the repair period. The repair is now complete, and the temporary laptop has been returned. However, the next user of the temporary laptop has found a number of websites that include a saved username and password from the previous user. Which of the following would be the BEST way to remove the saved account information from the previous user?

- A.** Delete all local usernames in User Accounts
- B.** Modify the information stored in Sync Center
- C.** Delete the saved account information using Credential Manager
- D.** Start the laptop in Safe Mode and login with an Administrator account
- E.** Delete any restore points in System Protection

Quick  
Answer: **161**

The Details: **218**

**B54.** A user has noticed that their mouse arrow has been moving around the screen without any user intervention. The user has seen the mouse opening and closing applications and changing settings in the Control Panel. Which of the following would be the BEST way for an administrator to resolve this issue?

- A.** Turn the firewall off and back on again
- B.** Run an anti-virus scan
- C.** Remove all recently installed applications
- D.** Upgrade to the latest OS patches

Quick  
Answer: **161**

The Details: **220**

- B55.** A server administrator has been planning an operating system upgrade for a group of important services. The administrator has provided a detailed scope and risk assessment of the change, and the plan has been documented. However, the end-user acceptance approvals weren't completed until Friday afternoon, so the change cannot occur over the weekend. Which of the following is preventing the upgrade from occurring?
- A. Upgrade file availability
  - B. Change board approval
  - C. Not enough time to complete the upgrade
  - D. Need more people for the upgrade process
- B56.** A user receives a browser security alert on his laptop when visiting any website that uses HTTPS. If he uses his smartphone, he does not receive any error messages. Which of the following would BEST describe this situation?
- A. The date and time on the laptop is incorrect
  - B. The smartphone is not updated with the latest OS version
  - C. The laptop has an incorrect subnet mask
  - D. The laptop does not have the latest anti-virus signatures
- B57.** A user on the sales team has opened a help desk ticket because of short battery times on a new company-provided tablet. When using the tablet, the battery only lasts a few hours before shutting off. Which of the following would be the BEST choices for improving the battery life? (Select TWO)
- A. Install the latest operating system patches
  - B. Increase the brightness levels
  - C. Connect to the corporate VPN
  - D. Disable Bluetooth and cellular connections
  - E. Close apps that work in the background
  - F. Perform a soft reset

Quick  
Answer: **161**

The Details: **221**

Quick  
Answer: **161**

The Details: **222**

Quick  
Answer: **161**

The Details: **223**

**B58.** A system administrator would like to perform a Windows installation while users are away from their desks. Which of the following would be the BEST option for this installation?

- A.** Unattended install
- B.** Multiboot
- C.** Repair installation
- D.** In-place upgrade

Quick  
Answer: **161**

The Details: **224**

**B59.** Walter, a user in the accounting department, has opened a help desk ticket that complains of garbled output from the local network printer. Any spreadsheet sent to the printer results in a jumble of text and graphics instead of the spreadsheet output. Which of the following should be the FIRST troubleshooting step?

- A.** Roll back to a previous operating system version
- B.** Stop and restart the network spooler service
- C.** Print a test page from the printer console
- D.** Perform a repair installation of the spreadsheet software

Quick  
Answer: **161**

The Details: **225**

**B60.** A macOS user needs to access a Windows application for a portion of their work day. Which of the following would be the BEST way to use this application?

- A.** Spaces
- B.** Remote Disc
- C.** Boot Camp
- D.** Spotlight

Quick  
Answer: **161**

The Details: **226**

**B61.** A data center manager is installing a new access door that will require multi-factor authentication. Which of the following should be used to meet this requirement? (Select TWO)

- A.** Cabinet locks
- B.** PIN input pad
- C.** Privacy filter
- D.** Handprint reader
- E.** USB lock
- F.** Cable lock

Quick  
Answer: **161**

The Details: **227**

**B62.** A user has opened a help desk ticket regarding the battery life in her three-year old smartphone. If a power source is not available, the phone battery is usually depleted by the middle of the work day. She uses the smartphone to access resources across the VPN, send and receive email, and run company-related apps. Her average screen time during the day usually exceeds ten hours. Which of the following would be the MOST likely reason for this battery issue?

- A.** The phone is consuming more power than usual
- B.** The battery capacity is decreased
- C.** The company apps need to be updated
- D.** The LCD screen is faulty

Quick  
Answer: **161**

The Details: **228**

**B63.** A desktop administrator has identified and removed malware on a corporate desktop computer. Which of the following malware removal steps should be performed NEXT?

- A.** Disconnect the computer from the corporate network
- B.** Educate the end-user
- C.** Schedule periodic anti-virus scans
- D.** Disable System Restore

Quick  
Answer: **161**

The Details: **229**

**B64.** Daniel, a graphics designer, has been editing large image files. He has found the process of saving these files on his hard drive has been taking longer over the last few weeks, but the file sizes haven't significantly changed. A technician checked the local resources and found that CPU and memory utilizations are low. Which of the following would be the best NEXT troubleshooting step?

- A.** Replace all system RAM
- B.** Defragment the hard drive
- C.** Roll back to a previous restore point
- D.** Perform a Windows Reset

Quick  
Answer: **161**

The Details: **230**

**B65.** A network administrator is installing a set of upgraded Internet routers in the data center. Which of the following would be the best choices to secure the access to the data center door? (Select TWO)

- A.** Biometric lock
- B.** USB lock
- C.** Locking cabinet
- D.** Privacy filter
- E.** Cable lock
- F.** Mantrap

Quick  
Answer: **161**

The Details: **231**

**B66.** An administrator is troubleshooting an error message that appears each time an application is started. The administrator has uninstalled and reinstalled the application, but the error message still appears. Which of the following would be the BEST next troubleshooting step?

- A.** Use Performance Manager to monitor the system
- B.** Check the Event Viewer logs
- C.** View the hardware settings in Device Manager
- D.** Disable unneeded background processes in Services

Quick  
Answer: **161**

The Details: **232**

**B67.** Daniel, a user in the accounting department, has received an email asking for payment of an outstanding invoice and a link to a third-party payment site. The email contains purchase information that appears to be correct, but additional research shows that the invoice number is not valid. Which of the following would BEST describe this attack type?

- A.** Spear phishing
- B.** Spoofing
- C.** Shoulder surfing
- D.** Man-in-the-middle

Quick  
Answer: **161**

The Details: **233**

- B68.** A user has dropped off their laptop at the repair desk. A message taped to the laptop states: "Doesn't work." Which of the following would be the BEST next step?
- A. Start the laptop and look for any issues
  - B. Call the customer and ask for more information
  - C. Replace the power adapter and try booting the laptop
  - D. Use a diagnostics boot CD to run hardware tests
- B69.** Which of these describes a free, open-source operating system?
- A. macOS
  - B. Linux
  - C. Windows
  - D. iOS
- B70.** An IT manager would like to provide users with the option to recover daily versions of documents and spreadsheets. A user will have the option to roll back to any daily version in the last month. Which of the following would be the BEST way to implement this feature?
- A. Create a file-level backup each day
  - B. Maintain a monthly image level backup
  - C. Store full backup tapes at an off-site facility
  - D. Assign each user a USB flash drive
- B71.** A network administrator has found that a daily report shows a single user with numerous visits to a website that violates the company's AUP. Which of the following should the administrator do NEXT?
- A. Create a firewall filter to block the website
  - B. Scan all computers with the latest anti-malware signatures
  - C. Contact the company's security officer
  - D. Change the user's password

Quick  
Answer: **161**

The Details: **234**

Quick  
Answer: **161**

The Details: **235**

Quick  
Answer: **161**

The Details: **236**

Quick  
Answer: **161**

The Details: **237**

**B72.** Which of the following script extensions would commonly be used inside of a Microsoft Office application?

- A. .vbs
- B. .py
- C. .bat
- D. .js

Quick  
Answer: **161**

The Details: **238**

**B73.** A system administrator has installed a SOHO network of five Windows computers. The administrator would like to provide a method of sharing documents and spreadsheets between all of the office computers. Which of the following would be the BEST way to provide this functionality?

- A. Domain
- B. Proxy server
- C. Workgroup
- D. Remote Desktop

Quick  
Answer: **161**

The Details: **239**

**B74.** A user took pictures of a new company product on their Apple tablet. Those pictures were posted on an industry rumor website the following week. Which of the following should be evaluated as the MOST likely security concern?

- A. iCloud
- B. OneDrive
- C. Google Sync
- D. iTunes

Quick  
Answer: **161**

The Details: **240**

**B75.** A manufacturing company in the United States provides monthly subscriptions and is storing customer credit card information for these recurring charges. Which of the following would be the MOST important set of policies to follow?

- A. GDPR
- B. PCI DSS
- C. EULA
- D. PHI

Quick  
Answer: **161**

The Details: **241**

**B76.** A user is traveling to a conference and they would like to be sure that any messages sent from their phone during the event remain private while using the event's wireless hotspot. Which of the following should be configured on this user's phone?

- A.** VPN
- B.** Strong password
- C.** Network-based firewall
- D.** Multi-factor authentication

Quick

Answer: **161**

The Details: **242**

**B77.** A company is installing a new wireless access point in a conference room. Which of the following would provide the BEST security for this network?

- A.** RC4
- B.** WPA2
- C.** TKIP
- D.** WEP

Quick

Answer: **161**

The Details: **243**

**B78.** A server administrator has configured an automated process to backup VM snapshots each evening during non-working hours. The backups will be stored on a series of high-density tape drives. How can the administrator confirm that these backups will be useful when a server recovery is needed?

- A.** Send the backups to an off-site facility
- B.** Connect the tape drives to a UPS
- C.** Create separate file-level backups
- D.** Perform occasional recovery tests

Quick

Answer: **161**

The Details: **244**

**B79.** A system administrator needs to configure a laptop to support inbound Remote Desktop services for the help desk team. Which of these Control Panel applets provides access to these settings?

- A.** Internet Properties
- B.** Devices and Printers
- C.** Network and Sharing Center
- D.** System

Quick

Answer: **161**

The Details: **245**

**B80.** A user has dropped off a laptop to the help desk and states that the laptop is experiencing a problem during the boot process. Which of these options would be the best path to resolve this issue?

- A.** When the customer provides enough information, stop them and let them know when they can pick up the laptop
- B.** Take the laptop and tell the customer to return tomorrow
- C.** Repeat an understanding of the issue back to the customer for verification
- D.** Provide recommendations to the customer with proper technical IT explanations

Quick  
Answer: **161**

The Details: **246**

**B81.** A technician is upgrading the motherboard in a server. Which of the following should be the FIRST task when beginning this upgrade?

- A.** Wear safety goggles
- B.** Connect an ESD strap
- C.** Remove any motherboard batteries
- D.** Disconnect from all power sources

Quick  
Answer: **161**

The Details: **247**

**B82.** A system administrator is installing a new video editing application on a user's workstation from an installation DVD-ROM. However, the installation process fails due to lack of available drive space. Which of the following would be the BEST way to complete the installation process?

- A.** Use a USB drive for the installation source
- B.** Compress the installation files
- C.** Install the application to a network share
- D.** Manually copy the installation files to the application directory

Quick  
Answer: **161**

The Details: **248**

**B83.** A user would like to install an image and photo editing program on their home computer, but they would prefer an application that did not require a monthly subscription. Which of the following would be the BEST licensing option for this requirement?

- A.** FOSS
- B.** Enterprise
- C.** Personal
- D.** Site

Quick  
Answer: **161**

The Details: **249**

**B84.** A system administrator is troubleshooting an issue with an application. The application uses an increasing amount of memory until all available RAM is eventually depleted. The computer must be rebooted every few days when this memory issue occurs. Which of the following utilities would show how much RAM is used by this application?

- A.** Event Viewer
- B.** Device Manager
- C.** Task Manager
- D.** Programs and Features

Quick  
Answer: **161**

The Details: **250**

**B85.** An administrator is troubleshooting a desktop computer that is experiencing a reboot loop. Before the Windows login screen appears, the system reboots in a continuous loop. Which of the following would be the BEST way to address this issue?

- A.** Start Safe Mode and perform a defragmentation
- B.** Reinstall the operating system from the original media
- C.** Update the boot order from the system BIOS
- D.** Run Startup Repair from the Advanced Boot Options

Quick  
Answer: **161**

The Details: **251**

**B86.** A user has downloaded a browser add-on that assists with new car purchases. During the installation, the Windows UAC is requesting administrative permissions to continue with the install. Which of these is the MOST likely situation?

- A.** The operating system requires an update
- B.** The software is a Trojan horse
- C.** The workstation is already part of a botnet
- D.** A worm will be downloaded and installed

Quick  
Answer: **161**

The Details: **252**

**B87.** An organization has distributed new laptops to all of their home-office employees. Although the users at home can successfully connect through the Internet to resources at the corporate office, there have been complaints that printers and shared drives at home are not accessible. Which of the following would explain this issue?

- A.** Incorrect login credentials
- B.** Port security is turned on
- C.** The corporate VPN is enabled
- D.** Blocked by DLP

Quick  
Answer: **161**

The Details: **253**

**B88.** A user on the marketing team is experiencing slower load times and ongoing sluggishness with applications on their laptop. A technician examines the Windows Update logs and finds that the monthly updates are failing. Which of the following should be the best NEXT step for resolving this issue?

- A.** Perform an anti-malware scan
- B.** Install the Windows Updates manually
- C.** Increase the amount of RAM in the laptop
- D.** Re-install the applications

Quick  
Answer: **161**

The Details: **254**

- B89.** A desktop administrator is troubleshooting an error that randomly causes a workstation to spike to 100% utilization. Which of these utilities would help the administrator track and report on system utilization over a 24-hour period?
- A.** Performance Monitor
  - B.** Device Manager
  - C.** Services
  - D.** Task Scheduler
- B90.** Which of these would be the BEST way to prevent an attacker from modifying default routes on a SOHO wireless network?
- A.** Configure MAC address filtering
  - B.** Enable WPS connectivity
  - C.** Change the router's default password
  - D.** Disable unneeded interfaces

Quick  
Answer: **161**

The Details: **255**

Quick  
Answer: **161**

The Details: **256**





# **Practice Exam B**

## **Multiple Choice Quick Answers**

- |              |              |        |
|--------------|--------------|--------|
| B6. A        | B36. B       | B66. B |
| B7. A        | B37. D       | B67. A |
| B8. B        | B38. A       | B68. B |
| B9. D        | B39. B       | B69. B |
| B10. C       | B40. A       | B70. A |
| B11. B       | B41. A       | B71. C |
| B12. D       | B42. D       | B72. A |
| B13. D       | B43. C       | B73. C |
| B14. B       | B44. D       | B74. A |
| B15. D       | B45. D       | B75. B |
| B16. C       | B46. D       | B76. A |
| B17. C       | B47. A       | B77. B |
| B18. B       | B48. B       | B78. D |
| B19. C and F | B49. B       | B79. D |
| B20. C       | B50. D       | B80. C |
| B21. A       | B51. A       | B81. D |
| B22. D       | B52. D       | B82. C |
| B23. B       | B53. C       | B83. A |
| B24. C       | B54. B       | B84. C |
| B25. A       | B55. B       | B85. D |
| B26. C       | B56. A       | B86. B |
| B27. B       | B57. D and E | B87. C |
| B28. A       | B58. A       | B88. A |
| B29. B       | B59. C       | B89. A |
| B30. B       | B60. C       | B90. C |
| B31. B       | B61. B and D |        |
| B32. D       | B62. B       |        |
| B33. A       | B63. C       |        |
| B34. D       | B64. B       |        |
| B35. C       | B65. A and F |        |



# Practice Exam B

## Detailed Answers

**B1.** Match the Windows utility to the function.

Some functions will not have a match.

### Commands:

### Descriptions:

Services	Disable a background process
----------	------------------------------

The Windows Services utility allows the system administrator to start, stop and manage all of the functions of a background process.

Performance Monitor	View the long-term CPU utilization of a server
---------------------	--

Performance Monitor can gather long-term statistics of OS metrics, set alerts and automated actions, store statistics, and display built-in reports.

Device Manager	View the version number of a device driver
----------------	--

All hardware is managed through the Windows Device Manager. Device drivers and hardware configurations can be managed through the Device Manager utility.

Event Viewer	View the logs associated with an application
--------------	--

The Windows Event Viewer is a central log consolidation tool for applications, security events, setup messages, and system details.

### Unused functions:

Task Scheduler	Schedule a batch file to run at 3 AM
----------------	--------------------------------------

The Windows Task Scheduler allows the user or administrator to run scripts or applications at designated times.

Windows Update

Update Windows system files

Windows Update is a centralized update utility that manages the patching of the operating system, drivers, and other important system files.

ODBC Data Sources

Create a database link to an external server

The ODBC (Open Database Connectivity) Data Sources utility integrates Windows applications with database services.



**More information:**

220-1002, Objective 1.5 - Windows Administrative Tools

<https://professormesser.link/1002010501>

---

- B2.** A network administrator is troubleshooting an intermittent Internet link outage to a server at 8.8.8.8. The administrator believes that the outage is occurring on one of the WAN connections between locations. Use a Windows network utility that can identify the router that is closest to the outage.



```
C:\Users\james>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  10.1.10.1
 2  9 ms     7 ms     8 ms  96.120.58.137
 3  7 ms     8 ms     7 ms  96.110.208.117
 4  8 ms     8 ms     9 ms  ae-11-ar01.mckeithen.fl.tallah.comcast.net [68.85.236.65]
 5  29 ms    27 ms    27 ms  be-33666-cr02.dallas.tx.ibone.comcast.net [68.86.90.221]
 6  26 ms    30 ms    31 ms  be-12495-pe03.1950stemmons.tx.ibone.comcast.net [68.86.85.194]
 7  27 ms    28 ms    27 ms  as15169-1-c.11ieighthave.ny.ibone.comcast.net [23.30.206.122]
 8  27 ms    27 ms    28 ms  108.170.231.44
 9  26 ms    27 ms    28 ms  108.170.231.69
10  27 ms    26 ms    26 ms  dns.google [8.8.8.8]

Trace complete.

C:\Users\james>
```

The tracert (traceroute) command will display a list of all network hops between two devices. If a route is down, the traceroute output will show the last hop before the faulty link.



#### More information:

220-1002, Section 1.4 - Network Command Line Tools  
<https://professormesser.link/1002010402>

**B3.** Match the scripting language with the most common use.

Some uses will not have a match.

### **Scripting**

**Language:**

**Use:**

VBScript	Import data into an Excel spreadsheet
----------	---------------------------------------

VBScript (Microsoft Visual Basic Scripting Edition) can be used for many Windows-related scripting purposes, but one of the most common is to automate the functionality of Microsoft Office applications.

JavaScript	Add animation to a website login screen
------------	---

JavaScript is used on many web sites to enhance the functionality within a user's browser. This can be used for automation, tracking, interactivity features, and to extend the functionality of the browser.

Python	Retrieve statistics from a network device
--------	---

Python is a scripting language that can handle almost anything, including a number of tasks in this list. However, Python is the best fit for a scripting language that can inter-operate with other devices, including devices across the network.

Batch file	Compare files on a Windows workstation
------------	--

A batch file commonly runs in the console or command line of a Windows device, and it can automate the same processes that a user would perform manually at the Windows command prompt.

## Unused options:

Shell script

Move log files on a Linux server

A shell script commonly runs at the command prompt, or shell, of a Unix or Linux device. Since most Linux features can be managed from the command line, shell scripts are very powerful automation options.

PowerShell

Disable an Active Directory account

PowerShell is a Windows-only scripting environment that extends the functionality of the traditional Windows command line. PowerShell extends the functionality of the command prompt to enable the automation of internal Windows and Active Directory functions.



### More information:

220-1002, Objective 4.8 - Scripting

<https://professormesser.link/1002040801>

---

- B4.** Select the Windows 10 Editions that include the following features.  
Some features will be included in multiple Windows 10 Editions:

Domain Membership

Pro

Enterprise

Connecting to a Windows Domain isn't something you would commonly see on a Home computer, so that feature is only available in Windows 10 Pro and higher editions.

AppLocker

Enterprise

AppLocker allows an administrator to manage which applications can run on company computers. This feature is only available in Windows 10 Enterprise.

BitLocker

Pro

Enterprise

BitLocker encrypts the entire volume in the Windows operating system, but this feature is not fully implemented in the Home edition of Windows 10.

BranchCache

Enterprise

Network administrators use BranchCache to store often-used files at a local site instead of transmitting them across the network each time they're used. This feature is only available in Windows 10 Enterprise edition.

Hyper-V

Pro

Enterprise

Hyper-V allows users to run multiple operating systems as virtual machines in Windows 10. This feature is included in Windows 10 Pro and higher.



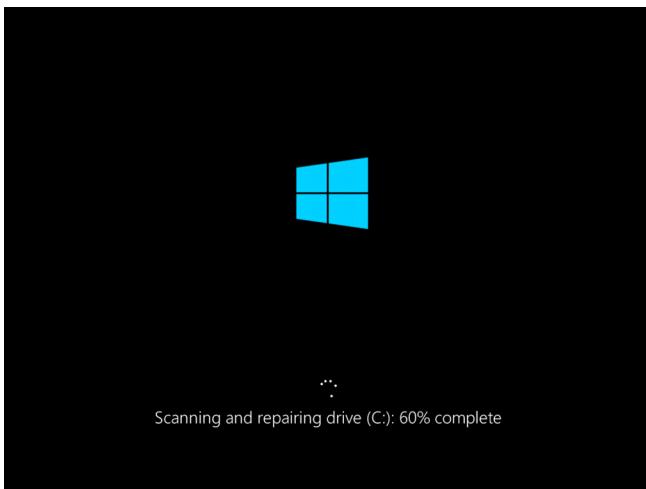
**More information:**

220-1002, An Overview of Windows 10

<https://professormesser.link/1002010203>

- B5.** A system administrator is concerned that the local Windows file system may contain logical file system errors. Scan and repair any potential file system errors from the Windows command line.

The chkdsk (Check Disk) command is used to identify and fix logical file system errors and bad physical sectors. The /f option will fix the logical file system and the /r option will locate bad sectors and attempt to recover any readable data. The scanning and repair process is often completed during a reboot:



**More information:**

220-1002, 1.4 - Microsoft Command Line Tools

<https://professormesser.link/1002010401>

---

**B6.** A technician is delivering a new laptop to a user and moving the older laptop to a different user. Which of the following would allow the existing hard drive to be used but prevent recovery of any of the previous user's data?

- A.** Regular format
  - B.** Run a defragmentation
  - C.** Connect the laptop to the Windows Domain
  - D.** Delete the \Users folder
- 

**The Answer:** **A.** Regular format

A regular format in Windows will overwrite each sector with zeros and prevent data recovery.

**The incorrect answers:**

**B.** Run a defragmentation

Although a defragmentation can overwrite some data, there's no guarantee that defragmenting the drive will result in overwriting all of the data. Recovery software may still be able to undelete data after a defragmentation has completed.

**C.** Connect the laptop to the Windows Domain

Associating a device to the Windows Domain allows it to be centrally managed, but it does not provide it with any protection of data on the hard drive.

**D.** Delete the \Users folder

The standard delete command in Windows does not overwrite any data on the hard drive. Recovery software can be used to view and save the previously deleted data.



**More information:**

220-1002, Objective 2.9 - Data Destruction and Disposal

<https://professormesser.link/1002020901>

- B7.** A desktop technician is replacing all of the CRT displays on a manufacturing line and replacing them with LCD displays. Which of the following would be the BEST way to dispose of the old monitors?
- A.** Take to a hazardous waste facility
  - B.** Return to the manufacturer
  - C.** Separate the parts and dispose of normally
  - D.** Contract with an incineration company
- 

**The Answer:** **A.** Take to a hazardous waste facility

The glass in a CRT (Cathode-Ray Tube) can contain lead, so it's important to dispose of those older displays at a local hazardous waste facility.

**The incorrect answers:**

**B.** Return to the manufacturer

The manufacturer of the equipment does not have a responsibility to accept old product returns. Once the equipment is purchased, it's the owner's responsibility to properly dispose of the equipment.

**C.** Separate the parts and dispose of normally

There's no need to separate the parts inside of a CRT, and some CRTs could potentially shock or electrocute someone touching the internal components. Even if the CRTs were dismantled, they would not be thrown out with the normal trash.

**D.** Contract with an incineration company

CRTs should not be incinerated, and instead should be properly disposed of at a local hazardous waste utility.



**More information:**

220-1002, Objective 4.4 - Safety Procedures

<https://professormesser.link/1002040401>

**B8.** A user needs to modify a spreadsheet for an upcoming meeting. The spreadsheet is currently stored on a remote computer in a shared drive. The user would like to access the shared drive as a drive letter inside of Windows File Explorer. Which of the following command line options would provide this functionality?

- A.** tasklist
  - B.** net use
  - C.** diskpart
  - D.** netstat
- 

**The Answer:** **B.** net use

The net use command will assign a local drive letter to a network share. Once the net use command is completed, the drive letter can be used to reference the share in all applications and in the File Explorer.

**The incorrect answers:**

**A.** tasklist

The tasklist command will display a list of all running processes in the operating system. The tasklist command will not associate a drive letter with a Windows share.

**C.** diskpart

The diskpart command is used to manage disk configurations, partitions, and volumes. The diskpart command is not used for drive letters and shares.

**D.** netstat

The netstat utility will display network statistics relating to active connections, application usage, and network activity. The netstat command does not associate drive letters with Windows shares.



**More information:**

220-1002, Objective 1.4 - Network Command Line Tools

<https://professormesser.link/1002010402>

- B9.** A macOS server administrator needs a backup system that will allow the recovery of data from any point in the last thirty days. Which of the following should be used for this requirement?
- A.** Backup and Restore
  - B.** Boot Camp
  - C.** Spaces
  - D.** Time Machine
- 

**The Answer:** **D.** Time Machine

The backup utility included with macOS is called Time Machine. Time Machine will create backups automatically and maintain as many days as the backup media's free space can store.

**The incorrect answers:**

**A.** Backup and Restore

The Windows backup utility is called Backup and Restore. These backups are not compatible with the macOS operating system.

**B.** Boot Camp

The Boot Camp utility allows the computer to dual boot between macOS and Windows. Boot Camp does not provide any backup or restore functionality.

**C.** Spaces

The Spaces utility can be used in macOS to create multiple desktops and separate work "spaces" that can be used independently of each other.



**More information:**

220-1002, Objective 1.9 - macOS Tools

<https://professormesser.link/1002010902>

**B10.** Why would a technician use an ESD strap?

- A. Protects electronic parts from extreme heat
  - B. Keeps electronic parts dry and free from moisture
  - C. Prevents damage from static electricity
  - D. Protects computer parts from dust
- 

**The Answer:** C. Prevents damage from static electricity

An ESD (Electrostatic Discharge) strap, or anti-static strap, connects a person to the equipment that they are working on. This commonly connects a wire from a user's wrist to a metal part on the computer or device.

**The incorrect answers:**

A. Protects electronic parts from extreme heat

An ESD strap does not provide any protection for extreme heat or temperature.

B. Keeps electronic parts dry and free from moisture

An anti-static strap does not provide any protection from the elements, so it would not be used to protect against moisture or water.

D. Protects computer parts from dust

Anti-static straps do not cover or protect computer components, so it would not protect a system from dust or debris.



**More information:**

220-1002, Objective 4.4 - Managing Electrostatic Discharge

<https://professormesser.link/1002040402>

**B11.** A desktop administrator is upgrading an older computer to support the 64-bit version of Windows 10 Pro. The computer currently has:

- 1 GHz CPU
- 1 GB of RAM
- 50 GB of free storage space
- 1024 x 768 video resolution

Which of the following should be upgraded to support the Windows 10 installation?

- A.** CPU
  - B.** RAM
  - C.** Storage space
  - D.** Video resolution
- 

#### **The Answer: B. RAM**

The 64-bit version of all Windows 10 editions require a minimum of 2 GB of system memory. Since this system only has 1 GB of RAM, it will need a memory upgrade before Windows 10 x64 can be installed.

#### **The incorrect answers:**

##### **A. CPU**

A processor running at 1 GHz is supported by both the 32-bit and 64-bit versions of Windows 10.

##### **C. Storage space**

The 64-bit version of Windows 10 requires 20 GB of free disk space. This system has 50 GB of free storage space, so it can easily support an upgrade to Windows 10 Pro x64.

##### **D. Video resolution**

Windows 10 Pro x64 requires a video resolution of 800 x 600, and this system supports a resolution of 1024 x 768 pixels.



#### **More information:**

220-1002, Objective 1.2 - An Overview of Windows 10

<https://professormesser.link/1002010203>

**B12.** Jack, a technician, is scheduled to replace a faulty motherboard today, but the motherboard delivery has been delayed and will not arrive until tomorrow. The new motherboard will repair a laptop used by a company executive. Which of the following would be the BEST way to handle these events?

- A. Move the installation to the next business day
  - B. Schedule another repair into today's newly opened time slot
  - C. Ask the delivery company for a refund on the shipping charges
  - D. Contact the end user and inform them of the shipping issue
- 

**The Answer:** D. Contact the end user and inform them of the shipping issue

It's important to always maintain an open line of communication with everyone involved with a project. When the situation is running as expected, a simple update may be all that's necessary. If problems occur, however, the other participants may want to make alternative plans. It's up to the technician to manage this open line of communication.

**The incorrect answers:**

**A.** Move the installation to the next business day

Moving the scheduled installation to the next business day without any other input would not be the best way to manage this repair. If the repair was time-sensitive, moving the installation may be the worst way to proceed.

**B.** Schedule another repair into today's newly opened time slot

Before prioritizing another repair into the existing time, it would be useful to know if there might be another option for the customer rather than to wait a day for the delivery to arrive.

**C.** Ask the delivery company for a refund on the shipping charges

Although there may be a case for refunding the shipping information, the current problem that needs resolution is the motherboard repair. There will be time after the repair is completed to determine if the shipping process was properly managed.



**More information:**

220-1002, Objective 4.7 - Communication

<https://professormesser.link/1002040701>

**B13.** A system administrator has been tasked with locating all of the log files contained within an application folder. The folder currently contains over a thousand files, and only a portion of them have a .log extension. Which of these Windows commands would be the BEST way to find these files?

- A.** sfc
  - B.** ls
  - C.** tasklist
  - D.** dir
- 

**The Answer:** **D.** dir

The dir (directory) command will display a list of files from the command line. The command includes filtering options, so using "dir \*.log" would display all files in the current directory with a .log extension.

**The incorrect answers:**

**A.** sfc

The sfc (System File Checker) command will scan the integrity of all protected system files and correct any files that may have been changed since their installation. The sfc command will not display a list of files in the current directory.

**B.** ls

The ls (list) command is the Linux command to show a list of files in the current directory. The ls command does not work from a Windows command line.

**C.** tasklist

The tasklist command will display a list of currently running processes. The tasklist command does not display a list of files in the current directory.



**More information:**

220-1002, Objective 1.4 - Microsoft Command Line Tools

<https://professormesser.link/1002010401>

**B14.** A user runs a corporate app on their smartphone that downloads a database each time the app is started. This download process normally takes a few seconds, but today the download is taking minutes to complete. Which of the following should a technician follow as the best NEXT troubleshooting step?

- A. Disable Bluetooth
  - B. Run a network speed check
  - C. Evaluate the app with an app scanner
  - D. Check the cloud storage resource usage
- 

**The Answer:** B. Run a network speed check

Delays associated with the downloading process would initially indicate a problem with the network connection. A speed check would evaluate the network connectivity and provide a baseline for download speeds.

**The incorrect answers:**

A. Disable Bluetooth

The Bluetooth radio would not cause a delay in transmitting traffic across the 802.11 network or cellular network. It's unlikely that disabling Bluetooth would provide any change to the download speed.

C. Evaluate the app with an app scanner

This app is a corporate published app, so using a third-party app scanner to determine the safety and security of the app would be unnecessary.

D. Check the cloud storage resource usage

The resource usage of a cloud storage platform would not cause the delays with this app.



**More information:**

220-1002, Objective 3.5

Troubleshooting Mobile Device Security

<https://professormesser.link/1002030501>

**B15.** A system administrator is analyzing a problem with a USB flash drive on a Windows 10 computer. When the flash drive is inserted, the CPU utilization increases to 100%. The administrator would like to disable one of the computer's USB controllers for troubleshooting. Which of the following would provide this functionality?

- A.** Services
  - B.** Performance Monitor
  - C.** Event Viewer
  - D.** Device Manager
- 

**The Answer: D. Device Manager**

The Windows Device Manager provides access to the device drivers that manage the hardware on a computer. Individual drivers can be enabled, disabled, and managed from the Device Manager utility.

**The incorrect answers:**

**A. Services**

The Services utility manages background service processes in Windows. The Services utility does not manage or disable hardware components.

**B. Performance Monitor**

The Performance Monitor gathers long-term statistics and can alert or create reports for ongoing performance metrics. Performance Monitor does not manage hardware device drivers.

**C. Event Viewer**

The Event Viewer contains logs from the applications, operating system, and other services. Although the Event Viewer may provide additional details about this flash drive issue, the administrator would not manage the device drivers from the Event Viewer utility.



**More information:**

220-1002, Objective 1.5 - Windows Administrative Tools  
<https://professormesser.link/1002010501>

**B16.** A user is reporting that some apps launched on their mobile phone will show an error message and then disappear without starting. This problem occurs with a group of apps that are normally used during the work day. Which of the following tasks would be the FIRST step for troubleshooting this issue?

- A.** Install the previous version of the apps
  - B.** Connect the phone to a power source
  - C.** Power cycle the phone
  - D.** Disable the GPS radio
- 

**The Answer:** **C.** Power cycle the phone

Before making any application or configuration changes, it's useful to power cycle a smartphone to reset the operating system. If the problem continues, then additional changes might be considered.

**The incorrect answers:**

**A.** Install the previous version of the apps

There's no evidence that the current version of the apps is the root cause of the issue. Before making changes to the software, it would be useful to perform some non-invasive troubleshooting and information-gathering tasks.

**B.** Connect the phone to a power source

Lack of a power source would not commonly cause applications to fail. This would therefore not be the best first step for troubleshooting these application issues.

**D.** Disable the GPS radio

The GPS radio would not commonly cause an app to fail, so disabling the GPS would not commonly be the first troubleshooting step.



#### More information:

220-1002, Objective 3.4 - Troubleshooting Mobile Apps  
<https://professormesser.link/1002030401>

**B17.** A technician has been asked to power down and store a server that has been exploited by an external attacker. The legal department will be performing tests and gathering information from this server. Which of the following would be MOST important to ensure the integrity of the server data?

- A.** Report the server location to the proper channels
  - B.** Compile all support tickets associated with the server
  - C.** Maintain a chain of custody
  - D.** Take photos of the server in the storage room
- 

**The Answer:** **C.** Maintain a chain of custody

It will be important that the data on the server is not modified. To ensure that all activity can be tracked, a chain of custody should be maintained at all times.

**The incorrect answers:**

**A.** Report the server location to the proper channels

It's useful for everyone to know where the server is located, but providing that information to the proper channels doesn't ensure that the data on the server is not modified.

**B.** Compile all support tickets associated with the server

A list of server support tickets may be useful for the incident investigation, but it won't help to ensure the integrity of the existing data on the server.

**D.** Take photos of the server in the storage room

A photographic image of the server, regardless of its location, will not help maintain the integrity of the data on the server.



**More information:**

220-1002, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1002040601>

**B18.** Jack, a user, has opened a help desk ticket to remove malware from his laptop. A previous removal occurred two weeks earlier with a similar malware infection. Which of the following was missed during the first malware removal?

- A. Restart the computer
  - B. Educate the end-user
  - C. Enable System Protection
  - D. Quarantine infected systems
- 

**The Answer:** B. Educate the end-user

Of the available possible answers, this is the only one that would have resulted in a reinfection if not properly followed. The users aren't malware experts, and they may not realize that their actions can have a negative effect on their system. Spending some quality time explaining anti-malware best practices can help prevent future infections.

**The incorrect answers:**

**A. Restart the computer**

Restarting the computer is not a necessary step in the malware removal process, and it wouldn't cause the computer to be more susceptible to another malware infection.

**C. Enable System Protection**

Enabling System Protection after malware has been removed does not make it more likely to receive another infection.

**D. Quarantine infected systems**

The quarantine process would prevent other devices from infection.

Missing the quarantine process would not necessarily cause the original system to become infected again.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**B19.** Which of the following features would be found in Windows 10 Enterprise but not in Windows 10 Pro? (Choose TWO)

- A.** Domain membership
  - B.** BitLocker
  - C.** BranchCache
  - D.** Hyper-V
  - E.** Remote Desktop host
  - F.** AppLocker
- 

**The Answer:** **C.** BranchCache, and **F.** AppLocker

BranchCache provides a method of caching data at remote sites to save time and bandwidth, and AppLocker provides administrative control of what applications can run in Windows. Both features are available in Windows 10 Enterprise but not in Windows 10 Pro.

**The incorrect answers:**

**A.** Domain membership

The ability to connect to an Active Directory domain is available in Windows 10 Pro and higher editions.

**B.** BitLocker

The full disk encryption functionality of BitLocker is available in Windows 10 Pro and higher.

**D.** Hyper-V

Running virtual machines with Microsoft's Hyper-V is available in Windows 10 Pro and higher.

**E.** Remote Desktop host

A Windows desktop can be configured with the Remote Desktop service in Windows 10 Pro and higher editions.



#### More information:

220-1002, Objective 1.2 - An Overview of Windows 10  
<https://professormesser.link/1002010203>

**B20.** A medical research company is using laptop computers when visiting testing centers. The IT security team is concerned about a private medical data breach if a laptop is lost or stolen. Which of the following would be the BEST way to manage this issue?

- A. BIOS password
  - B. Authenticator app
  - C. Full disk encryption
  - D. Biometric authentication
  - E. Cable lock
- 

**The Answer:** C. Full disk encryption

Encrypting all of the data on the laptop storage drives would prevent access to any data if the laptops are lost or stolen.

**The incorrect answers:**

**A. BIOS password**

A BIOS password would prevent someone from booting the operating system, but the data would still be accessible if the storage drive was removed from the laptop and moved to another system.

**B. Authenticator app**

An authenticator app would provide another factor of authentication during the login process, but it would not provide any additional security for the data stored on the laptop drive.

**D. Biometric authentication**

Using biometrics during the authentication process would ensure that the proper users were logging in, but it would not protect the data if the drives were removed from the laptop.

**E. Cable lock**

A cable lock might help prevent the laptop from theft, but it would not provide any data protection if the laptop was lost or stolen.



#### More information:

220-1002, Objective 2.8 - Securing Mobile Devices

<https://professormesser.link/1002020801>

**B21.** A user would like to encrypt a small group of files in a shared folder without affecting other files on the drive. Which of the following would be the BEST way to accomplish this?

- A.** EFS
  - B.** Save the files "as Administrator"
  - C.** BitLocker
  - D.** Save the files with a dollar sign at the end of the filename
- 

### **The Answer:** A. EFS

EFS (Encrypting File System) allows a user to encrypt individual objects at the file system level. With EFS, a single file or group of files can be protected without encrypting any other items on the storage drive.

### **The incorrect answers:**

**B.** Save the files "as Administrator"

Windows includes the option to execute an application with Administrator rights, but saving files does not include this option. By default, files are saved using the rights and permissions of the current user and changing this option would not provide any encryption features.

**C.** BitLocker

BitLocker is a full disk encryption technology that protects all of the data on the volume. BitLocker does not provide a feature to encrypt a single file or group of files.

**D.** Save the files with a dollar sign at the end of the filename

Creating a Windows share with a dollar sign at the end of the share name will hide the share from a public list. Saving a filename with a dollar sign at the end does not provide any protection or encryption of the file.



### **More information:**

220-1002, Objective 2.6 - Windows Security Settings

<https://professormesser.link/1002020601>

**B22.** A mobile user has transitioned to using apps on their smartphone for all business tasks. To ensure that no data will be lost, the smartphone will need to have multiple backups each day. The user travels most of the time and rarely visits the home office. Which of the following would be the best way to provide these backups?

- A.** Connect an external USB drive
  - B.** Use incremental backups each night
  - C.** Connect the smartphone to a laptop
  - D.** Use a cloud backup service
- 

**The Answer:** **D.** Use a cloud backup service

Using a cloud backup service such as Apple iCloud or Google Drive provides an automated method to constantly backup all user data on the smartphone. If the phone is lost or stolen, the user can purchase a new smartphone and restore all of the data from the cloud.

**The incorrect answers:**

**A.** Connect an external USB drive

Most smartphones do not support a backup to USB. This option would also require the user to remember to connect the USB drive multiple times and day and to maintain access to the USB flash drive.

**B.** Use incremental backups each night

Running nightly backups would not provide ongoing backups throughout the business day.

**C.** Connect the smartphone to a laptop

Most smartphone operating systems support the creation of a local backup to a connected computer, but this would not provide backups automatically throughout the day and would require manual intervention by the user.



**More information:**

220-1002, Objective 2.8 - Securing Mobile Devices  
<https://professormesser.link/1002020801>

**B23.** A desktop administrator is moving an SSD from one laptop to another. Which of the following should be used to protect the SSD during the move?

- A.** Padded envelope
  - B.** Anti-static bag
  - C.** Box with foam filler
  - D.** Cloth wrap
- 

**The Answer:** **B.** Anti-static bag

An anti-static bag would protect the SSD from inadvertent ESD (Electrostatic Discharge) while the component was moved between locations.

**The incorrect answers:**

**A.** Padded envelope

A padded envelope would protect against bumps, but it wouldn't provide any protection for inadvertent static discharge. Since the SSD doesn't include any moving parts, the padded envelope would provide limited protection.

**C.** Box with foam filler

The SSD does not have any moving parts, so extensive protection against bumps and movement isn't necessary. It would be more important to protect the delicate electronics on the drive, and the foam filler does not generally provide any anti-static protection.

**D.** Cloth wrap

Cloth can create static electricity, making this option one of the worst for transporting electronic equipment and components.



**More information:**

220-1002, Objective 4.4 - Managing Electrostatic Discharge

<https://professormesser.link/1002040402>

**B24.** A user is performing a series of Google searches, but the results pages are displaying links and advertisements from a different website. This issue occurs each time a Google search is performed. The same Google search on a different computer results in a normal Google results page. Which of the following would resolve this issue?

- A. Run the search from Safe Mode
  - B. Install the latest operating system patches
  - C. Run a malware removal utility
  - D. Login as a different user
- 

**The Answer:** C. Run a malware removal utility

If the results page of one website is unexpectedly directing to a different site, then the browser has most likely been hijacked by malware. Running a malware removal tool would be the best option of the available choices.

**The incorrect answers:**

A. Run the search from Safe Mode

If malware has infected the system and hijacked the browser, then operating the same browser from Safe Mode would result in the same hijacked page result.

B. Install the latest operating system patches

Operating system patches would not commonly remove a malware infection, so the redirection would continue to occur after the OS update.

D. Login as a different user

The malware that infected the current user's browser is most likely associated with all users on the system. Authenticating as a different user would not provide any resolution to this browser hijack.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues

<https://professormesser.link/1002030201>

**B25.** Jack, a user in the accounting department, is having an issue with his smartphone reaching websites and retrieving mail when working from home. Inside the office, the phone appears to work normally. Which of the following would be the best NEXT step for troubleshooting this issue?

- A. Verify the network configuration at home
  - B. Install the latest operating system updates
  - C. Connect the phone to power when working at home
  - D. Restart the smartphone after arriving at home
- 

**The Answer:** A. Verify the network configuration at home

If the smartphone is working properly in the office, then the overall functionality of the smartphone is working as expected. Since the issue is related to both websites and email, the focus should move to the network and the configuration the user has on their home network.

**The incorrect answers:**

B. Install the latest operating system updates

Since the smartphone works properly in the office, it would be unlikely that an operating system upgrade would resolve any problems at the user's home.

C. Connect the phone to power when working at home

Connecting to a power source doesn't provide any additional enhancements or connectivity options to websites or email servers.

D. Restart the smartphone after arriving at home

If the issue is not occurring in the office, then the smartphone is working as expected. Restarting the smartphone would not provide the most likely resolution to this issue.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**B26.** A security administrator has been asked to reinstall Windows on a web server diagnosed with a rootkit infection. Which of the following installation methods would be the BEST choice for this server?

- A.** In-place upgrade
  - B.** Multiboot
  - C.** Clean install
  - D.** Repair installation
- 

**The Answer:** **C.** Clean install

A clean install would be the best way to guarantee the removal of any malware. Leaving any portion of the operating system in place could potentially leave malware on the system.

**The incorrect answers:**

**A.** In-place upgrade

An in-place upgrade would change the operating system to a different version and would potentially leave malware running on the newly upgraded OS.

**B.** Multiboot

Multiboot is useful if two different operating systems needed to reside on the same computer. In this case, a single operating system is required and the rootkit needs to be completely removed.

**D.** Repair installation

A repair installation is designed to fix problems with the operating system and not to repair or remove any malware or rootkits. The only way to guarantee the removal of malware is to delete everything and reinstall or restore from a known good backup.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**B27.** A local coffee shop has a public wireless network for customers and a private wireless network for company devices. The shop owner wants to be sure that customers can never connect to the company network. Which of the following should be configured on this network?

- A.** Enable WPS on the customer network
  - B.** Configure WPA2 on the company network
  - C.** Require static IP addresses on the customer network
  - D.** Assign MAC filters to the company network
  - E.** Use a firewall between the customer and corporate network
- 

**The Answer:** **B.** Configure WPA2 on the company network

Enabling WPA2 (Wi-Fi Protected Access version 2) would require a password to connect and would prevent customers from connecting to the company wireless network.

**The incorrect answers:**

**A.** Enable WPS on the customer network

WPS (Wi-Fi Protected Setup) is used to simplify the connection process to a wireless network. WPS would not be used to prevent connectivity to an existing wireless network.

**C.** Require static IP addresses on the customer network

Requiring devices to configure their own static IP address adds additional administrative overhead without providing any security enhancement.

Static IP addressing does not prevent devices from connecting to a wireless network.

**D.** Assign MAC filters to the company network

MAC filtering can provide some administrative controls over access, but MAC filtering is not designed as a security control over wireless network access.

**E.** Use a firewall between the customer and corporate network

A firewall between networks would not prevent devices from connecting directly to a wireless network.



**More information:**

220-1002, Objective 2.10 - Securing a SOHO Network

<https://professormesser.link/1002021001>

**B28.** A user in the shipping department has logged into the Windows domain. However, the desktop does not show the user's normal wallpaper and all of the user's spreadsheets and documents in the "My Documents" folder are missing. Which of these would be the BEST way to restore the user's normal work environment?

- A. Rename the user's folder and delete their profile in the registry
  - B. Boot into Safe Mode and disable all startup applications
  - C. Add the user to the Administrator group
  - D. Update to the latest operating system version
- 

**The Answer:** A. Rename the user's folder and delete their profile in the registry

Problems with a user profile causes display problems on the desktop and user documents to disappear. To recreate the profile, the user's folder is deleted and the profile setting in the registry is deleted. Once the computer is restarted and the user logs in, a new profile will be created.

**The incorrect answers:**

B. Boot into Safe Mode and disable all startup applications

There's nothing associated with this issue that would indicate a problem with a startup application, and it would not be necessary to boot into Safe Mode if there was an issue with a startup application.

C. Add the user to the Administrator group

The user doesn't need administrator rights and permissions to load their own desktop and files. Adding the user to the Administrator group would not resolve the issue and would create a larger security concern.

D. Update to the latest operating system version

The current version of the operating system should properly load a user's profile and their documents. Updating the operating system would be a significant and unnecessary change.



#### More information:

220-1002, Objective 3.1 - Troubleshooting Solutions  
<https://professormesser.link/1002030102>

**B29.** A company's shipping department maintains ten different computers to print shipping labels and track outgoing shipments. All of the systems are displaying an error when they try to access a third-party shipping management website over a secure connection. Which of the following would be the MOST likely reason for this issue?

- A.** The computers have not been updated with the latest OS patches
  - B.** The website certificate has expired
  - C.** The local computer storage drives are not encrypted
  - D.** The systems are infected with malware
- 

**The Answer:** **B.** The website certificate has expired

All of the computers in the department were not able to connect to the third-party web site, so the problem does not appear to be associated with any single device. This points to the website as an issue, and the only available answer not associated with the local computers is a problem with the website encryption certificate.

**The incorrect answers:**

**A.** The computers have not been updated with the latest OS patches

Since the website operated normally before any operating system patches, it would not be necessary to install additional patches.

**C.** The local computer storage drives are not encrypted

The security of the local storage drives would not impact the computer's ability to properly browse to the third-party website.

**D.** The systems are infected with malware

A malware infection across all devices that cause them to fail in exactly the same way would be unusual, so this would not categorized as the most likely cause of this connectivity issue.



#### More information:

220-1002, Objective 3.2 - Troubleshooting Security Issues

<https://professormesser.link/1002030201>

**B30.** A manufacturing company performs a third-party audit of their accounting records each year. The auditors use laptops provided by the company to access internal resources. When the audit is complete, the auditors should be prevented from logging on until the following audit process begins. Which of the following would be the BEST way to accomplish this?

- A. Uninstall the audit software
  - B. Disable the accounts between audits
  - C. Remove the auditor accounts from all Windows groups
  - D. Require two-factor authentication for the auditor accounts
- 

**The Answer:** B. Disable the accounts between audits

The most secure option would prevent the auditor accounts from having any access to the network. The best way to prevent this access is to completely disable the accounts while they are not in use.

**The incorrect answers:**

A. Uninstall the audit software

Uninstalling the audit software doesn't prevent the auditor accounts from logging into the network or accessing other resources.

C. Remove the auditor accounts from all Windows groups

Removing the auditor accounts from the Windows groups does not prevent them from logging into the network, and it doesn't prevent those accounts from being added to other groups in the future.

D. Require two-factor authentication for the auditor accounts

Making the login process more difficult doesn't make it impossible.

Disabling the accounts would be the most secure, regardless of the number of authentication factors in use.



**More information:**

220-1002, Objective 2.7 - Workstation Security Best Practices

<https://professormesser.link/1002020701>

**B31.** A manufacturing company is donating some older computers to a local charity. Which of the following should be done to ensure that the existing hard drives could still be used but none of the existing data would be recoverable?

- A.** Degaussing
  - B.** Regular format
  - C.** Shredder
  - D.** Quick format
- 

**The Answer:** **B.** Regular format

The Windows operating system supports a quick format and a regular format. The regular format will overwrite every sector with zeros, which means that recovery software will not be able to restore any data on the drive.

**The incorrect answers:**

**A.** Degaussing

Degaussing will neutralize the magnetic field on the hard drive. This removes important startup information on the drive, causing the drive to no longer boot.

**C.** Shredder

Shredding the drives would physically destroy the drives, making them usable on the donated computers.

**D.** Quick format

The Windows Quick Format clears the drive index, but it doesn't overwrite any data on the drive. A recovery program could potentially restore all of the data after a quick format.



**More information:**

220-1002, Objective 2.9 - Data Destruction and Disposal

<https://professormesser.link/1002020901>

**B32.** A user's video editing workstation often performs an overnight rendering process. On some mornings, the user is presented with a login screen instead of the rendering completion page. A technician finds that the site occasionally loses power overnight. Which of the following should be used to avoid these issues with the video editing workstation?

- A.** Use a surge suppressor
  - B.** Save the rendered file to an external storage drive
  - C.** Create a separate partition for user documents
  - D.** Install a UPS
- 

**The Answer:** **D.** Install a UPS

A UPS (Uninterruptible Power Supply) can protect against brownouts, surges, and complete power blackouts. With a UPS, the video editing workstation would be protected against short-term overnight power problems.

**The incorrect answers:**

**A.** Use a surge suppressor

A surge suppressor protects against voltage spikes and line noise, but it doesn't provide any protection for a complete power outage.

**B.** Save the rendered file to an external storage drive

Saving the rendered file to a different drive doesn't provide any protection against a power outage, and the rendering would have to be restarted regardless of where the file was stored.

**C.** Create a separate partition for user documents

A separate partition would allow files to be organized differently, but it wouldn't provide any protection if primary power is lost.



**More information:**

220-1002, Objective 4.5 - Environmental Impacts

<https://professormesser.link/1002040501>

**B33.** A desktop administrator is troubleshooting an older computer that has been slowing down as more applications and files are stored on the hard drive. Which of the following commands would be the BEST choice for increasing the performance of this computer?

- A.** defrag
  - B.** format
  - C.** sfc
  - D.** mstsc
  - E.** dxdiag
- 

**The Answer:** **A.** defrag

As files are stored on a hard drive, the files can be fragmented and stored on different parts of the drive. The defragmentation utility moves the file fragments so they are contiguous, and this process improves the overall read and write times.

**The incorrect answers:**

**B.** format

The format command is used to initialize a file system. Running the format command would remove all of the information on the partition.

**C.** sfc

The sfc (System File Checker) utility will scan all protected system files and replace any files that may have changed since their installation.

**D.** mstsc

The mstsc (Microsoft Terminal Services Client) is the remote desktop client for Windows computers.

**E.** dxdiag

The dxdiag (DirectX Diagnostic Tool) is used to test the DirectX display, sound, and input devices on a Windows computer.



**More information:**

220-1002, Objective 1.5 - System Utilities

<https://professormesser.link/1002010506>

**B34.** A user in the accounting department has opened a help desk ticket regarding their email messages. There are reports of receiving unusual emails from the user, but the user has not sent any of these messages. A check of the unusual emails shows that they have been sent from the company's internal email server. Which of the following would be the best NEXT step in this troubleshooting process?

- A. Update the OS patches on the email server
  - B. Run an anti-malware utility on the systems that received the emails
  - C. Reimage the user's computer
  - D. Change the user's email password
- 

**The Answer:** D. Change the user's email password

If a user's account is being used to send messages from the corporate email server, then it's very likely that their email account information has been compromised. Before performing any additional troubleshooting, the best next step would be to change all of the user's corporate passwords.

**The incorrect answers:**

A. Update the OS patches on the email server

There's no evidence that the email server itself has been compromised, although it's always a good idea to maintain the latest server patches.

B. Run an anti-malware utility on systems that received the emails  
Simply receiving an email message does not automatically infect a device, so running anti-malware on the systems that received the email messages would not be the best next troubleshooting step.

C. Reimage the user's computer

It's quite possible that the user's account information was compromised without the involvement of the user's computer. Before making any significant hardware or software changes, it would be useful to change passwords and perform some additional investigation.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues  
<https://professormesser.link/1002030201>

**B35.** A system administrator has inadvertently installed a Trojan horse that has deleted a number of files across many Windows file shares. The Trojan also had access to user documents and login credentials and transmitted numerous documents to an off-site file storage system. Which of the following would limit the scope of future exploits?

- A.** Require multi-factor authentication
  - B.** Disable all guest accounts
  - C.** Modify the default permissions
  - D.** Configure full disk encryption
  - E.** Require complex passwords
  - F.** Require a screensaver password
- 

**The Answer:** **C.** Modify the default permissions

Many system administrators configure their accounts to have full access to the network as their default setting. This means that malicious software would also have full access if the administrator's desktop was exploited. Changing the default permissions to have limited access would also limit the scope of a Trojan horse exploit.

**The incorrect answers:**

**A.** Require multi-factor authentication

A Trojan horse exploit uses the permissions associated with the logged-in user. Requiring additional authentication factors will not have any effect on the scope of the malware infection.

**B.** Disable all guest accounts

Although disabling guest accounts is always a good best practice, the Trojan horse uses the current user permissions and does not require a guest account to function.

**D.** Configure full disk encryption

Full disk encryption protects the data on a storage drive if a device is lost or stolen. Once a user is logged in, the data can be accessed normally and the encryption is no longer a limitation to any user processes (such as a Trojan horse).

**E. Require complex passwords**

A complex password would protect against unauthorized user access, but it won't stop a Trojan horse from exploiting a system using the current user's account permissions.

**F. Require a screensaver password**

A screensaver password protects a system when the user is away from their desktop. A Trojan horse is executed by the user at an active workstation, so configuring a screensaver password would not protect against this infection.



**More information:**

220-1002, Objective 2.7 - Workstation Security Best Practices

<https://professormesser.link/1002020701>

**B36.** A technician has created an image that can be used across all of the computers in a training room. Which of the following would be the best way to deploy these images?

- A. Clean install
  - B. PXE
  - C. Repair installation
  - D. Multiboot
- 

**The Answer: B. PXE**

Using PXE (Preboot eXecution Environment), or "Pixie," a technician can boot computers from a centralized network server and automate the installation of multiple operating systems simultaneously.

**The incorrect answers:**

**A. Clean install**

A clean install requires separate installation media for each computer, so a room of thirty training computer will also require thirty separate installation boot media. PXE is a much more efficient method than using separate media.

**C. Repair installation**

A repair installation will overwrite an existing operating system with the same version. A repair installation does not use an image to reinstall the operating system.

**D. Multiboot**

Multiboot is a method of booting the system that displays a selection of multiple operating systems during the startup process. A multiboot system would not be a method of deploying operating systems in a training room.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**B37.** Which of the following Windows Share permissions has the priority when assigning access on a mapped drive?

- A. Allow
  - B. Full control
  - C. List folder contents
  - D. Deny
- 

**The Answer: D. Deny**

In Windows shares, the most restrictive setting has priority over all others. For example, the deny option takes priority over all other permissions.

**The incorrect answers:**

**A. Allow**

If a share is configured to deny access, it will take priority over an allow.

**B. Full control**

The permission option for full control would be configured for allow or deny access, and does not itself have priority over the deny option.

**C. List folder contents**

Listing folder contents is an NTFS permission that would be configured to allow or deny. These permission categories do not take priority over a deny setting.



**More information:**

220-1002, Objective 2.6 - Windows Security Settings

<https://professormesser.link/1002020601>

**B38.** A data center manager would like to ensure that a power fault on a server would not be harmful to employees. Which of the following would be the BEST choice for this requirement?

- A. Electrical ground
  - B. UPS
  - C. Air filter mask
  - D. ESD mat
- 

**The Answer:** A. Electrical ground

An electrical ground will divert any electrical faults away from people and into a copper grounding rod. An electrical ground is a critical part of any power system and equipment installation.

**The incorrect answers:**

**B. UPS**

A UPS (Uninterruptible Power Supply) provides a system with power if the main power source were to become unavailable. A UPS is not designed to protect people from an electrical shock.

**C. Air filter mask**

An air filter mask may be important for areas with dust or debris in the air, but it won't help protect people from inadvertent power faults or shorts.

**D. ESD mat**

An ESD (Electrostatic Discharge) mat is commonly used when working with the components inside of a computer, and its primary use is to prevent the discharge of static electricity. An ESD mat will not protect people from a main power fault on an electrical device.



**More information:**

220-1002, Objective 4.4 - Safety Procedures

<https://professormesser.link/1002040401>

**B39.** A user in the shipping department has received a call from someone claiming to be from the IT Help Desk. The caller asks the user to disclose their location, employee ID, and login credentials. Which of the following would describe this situation?

- A.** Denial of service
  - B.** Social engineering
  - C.** Brute force
  - D.** Man-in-the-middle
- 

**The Answer:** **B.** Social engineering

Someone claiming to be from an internal IT support department who knows nothing about an employees location or login credentials is most likely attempting to use the authority principle of social engineering to obtain private information.

**The incorrect answers:**

**A.** Denial of service

A denial of service is a process that prevents a service from operating normally. A caller asking private information is not causing a service to fail or be denied to others.

**C.** Brute force

A brute force attack describes the process of trial and error when attempting to reverse engineer an existing security feature. A caller asking questions would not be categorized as a brute force attack.

**D.** Man-in-the-middle

With a man-in-the-middle attack, a third party is able to intercept and listen to conversations between two other parties. An alleged IT Help Desk call is not categorized as a man-in-the-middle attack.



**More information:**

220-1002, Objective 2.5 - Social Engineering Attacks

<https://professormesser.link/1002020501>

**B40.** A desktop administrator has just removed malware from a user's desktop computer and has configured the system to automatically update anti-virus signatures and perform a scan each night. Which of the following should be the NEXT step in the removal process?

- A.** Enable System Protection
  - B.** Educate the end-user
  - C.** Quarantine the computer
  - D.** Boot to Safe Mode
- 

**The Answer:** **A.** Enable System Protection

Before the malware was removed, System Protection was disabled to delete all potentially-infected restore points. Once the malware is removed and the anti-malware process is working again, System Protection can be re-enabled.

**The incorrect answers:**

**B.** Educate the end-user

Once the malware is removed and all of the technical configurations are complete, the end-user can be educated on ways to identify and avoid a malware infection in the future.

**C.** Quarantine the computer

The quarantine process occurs immediately after malware has been identified. A technician would not wait until anti-malware configurations are complete before quarantining a system.

**D.** Boot to Safe Mode

Safe mode may be required during the malware removal process, but it's not necessary once the malware is removed and the anti-virus signatures are updated.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**B41.** A security administrator is installing a new VPN connection for remote users. The administrator would like all users to authenticate with their usual Windows Active Directory credentials. Which of the following technologies would provide this functionality?

- A. RADIUS
  - B. WPA2
  - C. TKIP
  - D. WEP
- 

**The Answer: A. RADIUS**

RADIUS (Remote Authentication Dial-in User Service) is an authentication protocol commonly used to provide authentication from devices to a centralized database. A common use of RADIUS is to authenticate users to an Active Directory database from a router, switch, VPN concentrator, or any other service.

**The incorrect answers:**

**B. WPA2**

WPA2 (Wi-Fi Protected Access version 2) is an 802.11 wireless security protocol. WPA2 would not be used to provide authentication features between devices and centralized databases.

**C. TKIP**

TKIP (Temporal Key Integrity Protocol) is a wireless protocol used with the original version of WPA. TKIP is not used to provide authentication to a centralized database.

**D. WEP**

WEP (Wired Equivalent Privacy) is an older wireless protocol that does not provide any authentication functionality to a centralized database.



**More information:**

220-1002, Objective 2.3 - Wireless Security

<https://professormesser.link/1002020301>

**B42.** Which of the following partition types limit a Windows installation to a maximum partition size of 2 TB?

- A. FAT32
  - B. GPT
  - C. NTFS
  - D. MBR
- 

**The Answer: D. MBR**

The MBR (Master Boot Record) partition style is an older method of partitioning files, and the maximum partition size of an MBR partition is 2 terabytes in size.

**The incorrect answers:**

**A. FAT32**

FAT32 (File Allocation Table 32-bit) is a Microsoft file system originally designed for earlier versions of Windows. FAT32 is not a partition type.

**B. GPT**

GPT (GUID Partition Table) is a modern partition style that increases the number of partitions and partition sizes over the older MBR style.

**C. NTFS**

NTFS (NT File System) is a Microsoft file system designed to replace the older FAT32 file system. NTFS is not a type of partition.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**B43.** A system administrator has just completed an update of fifty servers to the latest version of an application, and the updated software has been working as expected for the last three days. Which of the following change management steps should be followed NEXT?

- A.** Create a backout plan
  - B.** Determine the scope of the changes
  - C.** Document the changes
  - D.** Determine the risk for the upgrade process
- 

**The Answer:** **C.** Document the changes

After the final changes are complete, it's useful to document the process and the changes for future reference. The next technician who needs to perform a similar change can use this documentation as a point of reference and can use the documentation to avoid any issues that may have occurred during this update.

**The incorrect answers:**

**A.** Create a backout plan

A backout plan should be created prior to making any changes. If there are unexpected issues during the update process, the backout process can be followed to return the system to a functioning state.

**B.** Determine the scope of the changes

Determining the effect of the change is one of the first steps of the change control process. Understanding the scope of the proposed changes would not be very useful after the changes have been made.

**D.** Determine the risk for the upgrade process

Before making any changes, it's important to know what risks might exist for this update. The risk analysis is created well before the update process begins.



**More information:**

220-1002, Objective 4.2 - Change Management  
<https://professormesser.link/1002040201>

**B44.** A help desk technician has been tasked with rebuilding an email server that recently crashed. Which of the following would be the BEST source for this information?

- A.** Compliance report
  - B.** Acceptable use policies
  - C.** Network topology map
  - D.** Knowledge base
- 

**The Answer:** **D.** Knowledge base

A knowledge base commonly contains information about processes, procedures, and documentation for resolving technical issues. An internal knowledgebase would contain important historical information about the email server and would potentially document the hardware and software specifications for the server.

**The incorrect answers:**

**A.** Compliance report

A compliance report would document how closely the email server complied with a set of rules or regulations associated with the company or service. A compliance report might document how long email messages were stored and how they were protected, but it would not commonly contain the information required to rebuild the server.

**B.** Acceptable use policies

An acceptable use policy (AUP) describes the rules of behavior for users of the organization's services and equipment. An AUP does not contain any information that would assist with the rebuilding of an email server.

**C.** Network topology map

A network topology map would display the location of the email server in the organization's network, but it would not contain the information required to rebuild the hardware and software of the server.



**More information:**

220-1002, Objective 4.1 - Documentation Best Practices

<https://professormesser.link/1002040101>

**B45.** A server administrator is installing a 4 TB drive in a database server and would like to use the entire free space as a single partition. Which of the following technologies should be used with this drive?

- A.** FAT32
  - B.** MBR
  - C.** NFS
  - D.** GPT
- 

**The Answer: D. GPT**

The GPT (GUID Partition Table) partition style provides for very large partition sizes that would easily allow a single partition of 4 terabytes.

**The incorrect answers:**

**A. FAT32**

The FAT32 (File Allocation Table 32-bit) file system limits volume sizes to a maximum of 2 TB.

**B. MBR**

The MBR (Master Boot Record) partition style does not allow the creation of partitions greater than 2 TB.

**C. NFS**

NFS (Network File System) is a method of accessing files across the network as if they were local. NFS is not a method of partitioning a local storage drive.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**B46.** A user has called the help desk to get assistance with random blue screens on their Windows 10 laptop. The technician finds that CPU utilization is constantly high, and many network sites are unavailable or only load half of the site content. The user mentions that some random pop-up messages have appeared on the desktop during the workday. Which of the following would be the MOST likely reason for these issues?

- A.** Storage drive is failing
  - B.** Network proxy settings are incorrect
  - C.** Operating system needs to be updated
  - D.** Laptop has a malware infection
  - E.** Video subsystem is faulty
- 

**The Answer:** **D.** Laptop has a malware infection

Slow system performance, intermittent connectivity, and random pop-up messages are clear indications of a malware infection.

**The incorrect answers:**

**A.** Storage drive is failing

A failing storage drive may cause slowness and error messages, but it would not commonly cause network connectivity issues and random pop-up messages.

**B.** Network proxy settings are incorrect

Incorrect network proxy settings would usually cause all of the network communication to fail. An invalid proxy configuration would not commonly result in random pop-up messages.

**C.** Operating system needs to be updated

It's always a good idea to keep the operating system up to date, but an outdated OS would not have connectivity issues or display random pop-up messages.

**E.** Video subsystem is faulty

A bad video subsystem might cause a blue screen stop error, but there would also commonly be some type of visual issue with the video. A bad video subsystem would not commonly cause network issues or pop-ups.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1002030101>

**B47.** A technician is troubleshooting an issue with an iOS tablet randomly restarting during normal use. A check of the device shows there have been no significant application updates and the operating system was upgraded to a new version three days ago. The user states the tablet was working normally last week. Which of the following would be the MOST likely reason for these random reboots?

- A.** Faulty OS upgrade
  - B.** Invalid device certificate
  - C.** Malware infection
  - D.** Faulty battery
  - E.** Incorrect network settings
- 

**The Answer:** **A.** Faulty OS upgrade

The last change to the tablet was an upgrade just three days ago, and the tablet worked normally before that event. This documented change would be the most likely reason for this issue.

**The incorrect answers:**

**B.** Invalid device certificate

An invalid device certificate may cause authentication issues, but it would not cause the tablet to randomly restart.

**C.** Malware infection

Random reboots could possibly be caused by malware infections, but the documented OS upgrade is a more obvious change to the system.

**D.** Faulty battery

A faulty battery could be considered an issue if no other changes were made to the tablet and the tablet didn't restart after powering down.

**E.** Incorrect network settings

Incorrect network settings might cause connectivity issues to remote devices, but it wouldn't cause the tablet to randomly restart.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

- B48.** A system administrator needs to modify a file in the \Windows\Installer directory, but the folder doesn't appear in the file list. Which of these options would help the system administrator with this task?
- A.** Safe Mode
  - B.** File Explorer Options
  - C.** User Accounts
  - D.** Internet Options
- 

**The Answer:** **B.** File Explorer Options

The File Explorer commonly hides operating system files. Un-checking the "Hide protected operating system files (Recommended)" would display the files to the system administrator.

**The incorrect answers:**

**A.** Safe Mode

Safe Mode is useful when troubleshooting operating system problems, but it will not change the files displayed in Windows File Explorer.

**C.** User Accounts

The User Accounts Control Panel applet can be used to create or modify existing accounts. The User Accounts options do not include the ability to display or hide certain file types.

**D.** Internet Options

The Internet Options configuration can be used to modify the connectivity options available when using a browser. These options will not enable or disable the display of certain file types.



**More information:**

220-1002, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1002010601>

**B49.** A Linux administrator is modifying a log file and needs to rename the file. Which of the following should be used to make this change?

- A.** rm
  - B.** mv
  - C.** mkdir
  - D.** pwd
- 

**The Answer:** **B.** mv

The Linux mv (move) command will move a file from one location to another or move/rename a file from one name to another.

**The incorrect answers:**

**A.** rm

The Linux rm (remove) command will delete a file or object from the file system.

**C.** mkdir

The mkdir (Make Directory) command can be used in Linux or Windows to create a folder or directory in the file system.

**D.** pwd

The Linux pwd (Print Working Directory) command will display the path of the current working directory.



**More information:**

220-1002, Objective 1.9 - Basic Linux Commands

<https://professormesser.link/1002010906>

**B50.** A desktop administrator is troubleshooting poor performance on a user's laptop computer. The system takes an excessive amount of time during the boot process, and pop up messages appear while using the word processor and spreadsheet applications. Which of the following steps should the technician do NEXT?

- A.** Educate the end-user
  - B.** Schedule periodic anti-virus scans
  - C.** Enable System Protection
  - D.** Disconnect the laptop from the network
- 

**The Answer:** **D.** Disconnect the laptop from the network

Once malware has been suspected or identified, the first step is to quarantine the system from all other computers. The laptop should be disconnected from the network to prevent communication with other devices.

**The incorrect answers:**

**A.** Educate the end-user

The priority is to limit the scope of the malware and remove it from the system. Once the malware has been removed, it's important to discuss malware prevention and best practices with the user.

**B.** Schedule periodic anti-virus scans

After the malware has been removed, it's important to make sure the system is able to scan for any potential future infections.

**C.** Enable System Protection

System Protection is disabled before the malware is removed to erase any restore points that might also be infected. Once the malware is removed, this feature can be re-enabled.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**B51.** Jack, an executive, has a laptop that runs very slowly after login and continues running slowly throughout the day. Jack has complained that certain applications cannot be started and others will randomly crash. A check of the laptop shows that the memory utilization is very close to 100%. Which of the following would provide a short-term fix for this issue?

- A.** Disable startup items
  - B.** Update to the latest OS patches
  - C.** Defragment the hard drive
  - D.** Reboot the computer
- 

**The Answer:** **A.** Disable startup items

The memory utilization issue appears immediately after the login process, so disabling some startup items may help resolve the issue until a memory upgrade or better laptop is located.

**The incorrect answers:**

**B.** Update to the latest OS patches

The over-utilization of RAM isn't something that can be commonly resolved with an OS patch. The two best options are to add more RAM or to limit what runs in the current memory space.

**C.** Defragment the hard drive

There's no evidence that a fragmented hard drive would be causing these slowdowns, and the high utilization of RAM appears to indicate an issue with the memory resources available for the active applications.

**D.** Reboot the computer

Because this issue appears immediately after login, rebooting the system would not be the most likely short-term resolution for this memory issue.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1002030101>

**B52.** A help desk technician needs to view and control the desktop of a Windows computer at a remote location. Which of the following would be the BEST choice for this task?

- A.** Telnet
  - B.** VNC
  - C.** SSH
  - D.** RDP
- 

**The Answer: D. RDP**

The integrated Windows RDP (Remote Desktop Protocol) is used to view and control the screen of a remote computer.

**The incorrect answers:**

**A. Telnet**

Telnet is commonly used to manage the command line of a remote device. Telnet does not use any encryption, and most best practices would require SSH to manage a remote command line.

**B. VNC**

VNC (Virtual Network Computing) is a remote desktop application that is commonly associated with Linux and macOS desktop sharing. The best choice for a Windows computer is to use the built-in RDP services.

**C. SSH**

SSH (Secure Shell) is a secure terminal utility that can manage the command line of a remote device over an encrypted connection.



**More information:**

220-1002, Objective 4.9 - Remote Access Technologies  
<https://professormesser.link/1002040901>

**B53.** The storage drive in a user's laptop has recently failed, and a temporary laptop was assigned to the user during the repair period. The repair is now complete, and the temporary laptop has been returned. However, the next user of the temporary laptop has found a number of websites that include a saved username and password from the previous user. Which of the following would be the BEST way to remove the saved account information from the previous user?

- A. Delete all local usernames in User Accounts
  - B. Modify the information stored in Sync Center
  - C. Delete the saved account information using Credential Manager
  - D. Start the laptop in Safe Mode and login with an Administrator account
  - E. Delete any restore points in System Protection
- 

**The Answer:** C. Delete the saved account information using Credential Manager

The Windows Credential Manager can store web and Windows credentials, certificates, and other authentication details. The login details can be viewed and deleted from the Credential Manager.

**The incorrect answers:**

A. Delete all local usernames in User Accounts

Account name, type, passwords, pictures, and other information is stored in the User Accounts applet. Credential information cannot be modified from the User Accounts utility.

B. Modify the information stored in Sync Center

The Sync Center is used to provide access to offline files, and those files are automatically synchronized when reconnected to the network. Credential information is not stored in the Sync Center.

**D.** Start the laptop in Safe Mode and login with an Administrator account  
Logging on with an Administrator account does not remove any credentials that may be stored on a system, and Safe Mode does not change the functionality of the Administrator account.

**E.** Delete any restore points in System Protection

System Protection is used to recover the system configuration to a prior restore point. Deleting the previously saved restore points will not remove saved credentials from the current Windows configuration.



**More information:**

220-1002, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1002010601>

**B54.** A user has noticed that their mouse arrow has been moving around the screen without any user intervention. The user has seen the mouse opening and closing applications and changing settings in the Control Panel. Which of the following would be the BEST way for an administrator to resolve this issue?

- A.** Turn the firewall off and back on again
  - B.** Run an anti-virus scan
  - C.** Remove all recently installed applications
  - D.** Upgrade to the latest OS patches
- 

**The Answer:** **B.** Run an anti-virus scan

A system with a mouse that moves independently and opens applications and other windows is most likely infected with malware. The best available option is to run an anti-virus scan to determine the scope of the infection.

**The incorrect answers:**

**A.** Turn the firewall off and back on again

Since this issue appears to occur when the firewall is active, toggling the state of the firewall would not resolve this issue.

**C.** Remove all recently installed applications

Although it's possible that this malware infection was part of a recently installed application, it's now likely that the malware has infected other parts of the system. Uninstalling the applications would probably not remove the malware.

**D.** Upgrade to the latest OS patches

Keeping the operating system updated can often prevent malware infections. However, once the system is compromised, installing the latest patches will not resolve the existing infection.



**More information:**

220-1002, Objective 2.4 - Types of Malware

<https://professormesser.link/1002020401>

**B55.** A server administrator has been planning an operating system upgrade for a group of important services. The administrator has provided a detailed scope and risk assessment of the change, and the plan has been documented. However, the end-user acceptance approvals weren't completed until Friday afternoon, so the change cannot occur over the weekend. Which of the following is preventing the upgrade from occurring?

- A.** Upgrade file availability
  - B.** Change board approval
  - C.** Not enough time to complete the upgrade
  - D.** Need more people for the upgrade process
- 

**The Answer:** **B.** Change board approval

Before a change can proceed, the change board must evaluate and approve the proposal. Most of these boards meet well before the change date to make sure that all affected parties have a chance to evaluate the risk and understand the scope of the change. The users approved the plan on a Friday afternoon, but the change board did not have time to properly evaluate and approve the change process for the weekend schedule.

**The incorrect answers:**

**A.** Upgrade file availability

Since the upgrade plan was already written, it's most likely that all of the upgrade files were in place and ready.

**C.** Not enough time to complete the upgrade

This question didn't define a specific timeframe for completion, although it's common to complete changes during a weekend.

**D.** Need more people for the upgrade process

The question didn't define any personnel requirements, so there did not appear to be any constraints on the availability of personnel.



**More information:**

220-1002, Objective 4.2 - Change Management

<https://professormesser.link/1002040201>

**B56.** A user receives a browser security alert on his laptop when visiting any website that uses HTTPS. If he uses his smartphone, he does not receive any error messages. Which of the following would BEST describe this situation?

- A. The date and time on the laptop is incorrect
  - B. The smartphone is not updated with the latest OS version
  - C. The laptop has an incorrect subnet mask
  - D. The laptop does not have the latest anti-virus signatures
- 

**The Answer:** A. The date and time on the laptop is incorrect

The date and time on a device is important when encryption is involved. If a date is very different between devices, the encryption process may fail or the encryption certificate may appear to be expired.

**The incorrect answers:**

B. The smartphone is not updated with the latest OS version

The smartphone doesn't appear to have any issues with the encrypted website, so updating the smartphone would not resolve the encryption issue on the laptop.

C. The laptop has an incorrect subnet mask

An incorrect subnet mask might cause network connectivity issues, but it would not commonly cause an error with the browser encryption process.

D. The laptop does not have the latest anti-virus signatures

The anti-virus signatures on a device are not related to the browser encryption process.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues  
<https://professormesser.link/1002030201>

**B57.** A user on the sales team has opened a help desk ticket because of short battery times on a new company-provided tablet. When using the tablet, the battery only lasts a few hours before shutting off. Which of the following would be the BEST choices for improving the battery life? (Select TWO)

- A. Install the latest operating system patches
  - B. Increase the brightness levels
  - C. Connect to the corporate VPN
  - D. Disable Bluetooth and cellular connections
  - E. Close apps that work in the background
  - F. Perform a soft reset
- 

**The Answers:** D. Disable Bluetooth and cellular connections, and  
E. Close apps that work in the background

The two options that would have the largest power savings would disable wireless Bluetooth radios and close applications that use CPU power.

**The incorrect answers:**

A. Install the latest operating system patches

Installing operating system patches does not commonly resolve issues with excessive battery usage. After installing the patches, the battery use would most likely remain the same.

B. Increase the brightness levels

Increasing brightness levels would have the opposite of the intended effect, since additional battery will be required by the brighter display.

C. Connect to the corporate VPN

Connecting to the corporate VPN (Virtual Private Network) would require additional wireless communication and increased CPU usage due to the encryption and decryption process used by the VPN.

F. Perform a soft reset

Performing a soft reset might help if the issue was associated with a problematic application or unusual system state. There's no evidence that either of these is occurring, so resetting the system would most likely have no effect on the battery life.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**B58.** A system administrator would like to perform a Windows installation while users are away from their desks. Which of the following would be the BEST option for this installation?

- A.** Unattended install
  - B.** Multiboot
  - C.** Repair installation
  - D.** In-place upgrade
- 

**The Answer:** **A.** Unattended install

An unattended install uses a previously configured answer file instead of prompting the user to provide answers during the installation process. This allows the entire installation to occur without any user intervention and can be used when users are not available.

**The incorrect answers:**

**B.** Multiboot

A multiboot system is installed with multiple operating systems that can be selected during the boot process. A multiboot system does not itself provide a way to install Windows without user intervention.

**C.** Repair installation

A repair installation will overwrite an existing installation with the same version of the operating system in an effort to repair problems that may have occurred with the existing installation. A repair installation does not imply that the installation would be performed without user intervention.

**D.** In-place upgrade

An in-place upgrade will leave user documents and configurations in place during the upgrade process. An in-place upgrade does not imply that the installation would be performed without user intervention.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**B59.** Walter, a user in the accounting department, has opened a help desk ticket that complains of garbled output from the local network printer. Any spreadsheet sent to the printer results in a jumble of text and graphics instead of the spreadsheet output. Which of the following should be the FIRST troubleshooting step?

- A. Roll back to a previous operating system version
  - B. Stop and restart the network spooler service
  - C. Print a test page from the printer console
  - D. Perform a repair installation of the spreadsheet software
- 

**The Answers:** C. Print a test page from the printer console

It would be useful to know if the printer is working properly or if the issue occurred prior to the output reaching the printer. Printing a test page from the printer console circumvents the network, operating system, driver, and application to determine if the printer itself is working properly.

**The incorrect answers:**

A. Roll back to a previous operating system version

Changing the operating system doesn't usually have a significant effect on the printing process. Making such a significant change would not be the first troubleshooting step.

B. Stop and restart the network spooler service

If the printer was not printing at all, restarting the service would be a good first choice. In this example, the problem is with the output itself.

D. Perform a repair installation of the spreadsheet software

It's possible that the spreadsheet software might be part of the problem, but before making any changes it would be good to verify that the printer is currently in working order.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1002030101>

**B60.** A macOS user needs to access a Windows application for a portion of their work day. Which of the following would be the BEST way to use this application?

- A.** Spaces
  - B.** Remote Disc
  - C.** Boot Camp
  - D.** Spotlight
- 

**The Answer:** **C.** Boot Camp

The macOS Boot Camp feature allows a user to configure the Apple hardware to boot between macOS and Windows. The user can reboot into Windows for access to the application, and boot back to macOS when the task is completed.

**The incorrect answers:**

**A.** Spaces

Spaces allows a user to configured multiple macOS desktops on the screen. The Spaces feature does not allow the macOS desktop to run Windows applications.

**B.** Remote Disc

Remote Disc is a feature that allow a macOS user to share the optical drive of another computer on the network. Remote Disc does not provide a method of running Windows applications.

**D.** Spotlight

Spotlight is the built-in macOS search feature for locating files, applications, email messages, and more. Spotlight does not provide a method of running Windows applications.



**More information:**

220-1002, Objective 1.9 - macOS Features

<https://professormesser.link/1002010903>

**B61.** A data center manager is installing a new access door that will require multi-factor authentication. Which of the following should be used to meet this requirement? (Select TWO)

- A. Cabinet locks
  - B. PIN input pad
  - C. Privacy filter
  - D. Handprint reader
  - E. USB lock
  - F. Cable lock
- 

**The Answer:** **B.** PIN input pad and **D.** Handprint reader

The only two devices that provide authentication are the PIN (Personal Identification Number) and the handprint reader. The PIN is a factor of something you know, and the handprint reader is a factor of something you are.

**The incorrect answers:**

**A.** Cabinet locks

Cabinet locks are used to protect the information inside the data center cabinets and do not protect the access door to the data center itself.

**C.** Privacy filter

A privacy filter is used on a monitor or LCD screen to limit the ability for others to see the screen contents. A privacy filter would not provide authentication for an access door.

**E.** USB lock

A USB lock is used to secure access to the USB interfaces on a computer system. USB locks are not used for physical doorways.

**F.** Cable lock

A cable lock is used to securely attach a device to something solid to prevent theft. Cable locks are not used to secure entrance doors.



**More information:**

220-1002, Objective 2.2 - Logical Security

<https://professormesser.link/1002020201>

**B62.** A user has opened a help desk ticket regarding the battery life in her three-year old smartphone. If a power source is not available, the phone battery is usually depleted by the middle of the work day. She uses the smartphone to access resources across the VPN, send and receive email, and run company-related apps. Her average screen time during the day usually exceeds ten hours. Which of the following would be the MOST likely reason for this battery issue?

- A. The phone is consuming more power than usual
  - B. The battery capacity is decreased
  - C. The company apps need to be updated
  - D. The LCD screen is faulty
- 

**The Answer:** B. The battery capacity is decreased

Smartphone batteries have a lifespan of about 300 to 500 charge cycles, so smartphone that's three years old will not have the same capacity as the battery in a new smartphone.

**The incorrect answers:**

A. The phone is consuming more power than usual

This user does not appear to be doing anything differently than normal, and none of the apps on the phone appear to be using more power than usual.

C. The company apps need to be updated

None of the apps on the phone are experiencing any issues, and the overall battery usage appears to match the normal use. Upgrading the apps would most likely not resolve this power issue.

D. The LCD screen is faulty

There's no evidence that the LCD screen is having problems, and the battery usage of the smartphone does not appear to be related to any LCD issues.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**B63.** A desktop administrator has identified and removed malware on a corporate desktop computer. Which of the following malware removal steps should be performed NEXT?

- A.** Disconnect the computer from the corporate network
  - B.** Educate the end-user
  - C.** Schedule periodic anti-virus scans
  - D.** Disable System Restore
- 

**The Answer:** **C.** Schedule periodic anti-virus scans

After removing malware and before educating the end-user, it's important to configure the system to find and prevent any future infections.

**The incorrect answers:**

**A.** Disconnect the computer from the corporate network

Quarantining the system should be the first step after suspecting that a malware infection is on the computer. This process would not occur after malware was already removed.

**B.** Educate the end-user

After the system is repaired and set for automated protection, the end-user should be educated to help prevent this situation in the future.

**D.** Disable System Restore

The System Restore process is disabled before removing the malware to delete all potentially infected restore points on the computer.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**B64.** Daniel, a graphics designer, has been editing large image files. He has found the process of saving these files on his hard drive has been taking longer over the last few weeks, but the file sizes haven't significantly changed. A technician checked the local resources and found that CPU and memory utilizations are low. Which of the following would be the best NEXT troubleshooting step?

- A. Replace all system RAM
  - B. Defragment the hard drive
  - C. Roll back to a previous restore point
  - D. Perform a Windows Reset
- 

**The Answer:** B. Defragment the hard drive

As files are stored on a hard drive, they can be fragmented to different areas. This will cause delays as parts of the file have to be retrieved from different areas of the drive. Running a defragmentation won't change any files or configurations, but it will move the fragments so they are contiguous.

**The incorrect answers:**

A. Replace all system RAM

Faulty memory will cause a computer to halt or fail with no warning. In this case, there have been no issues related with the stability of the system.

C. Roll back to a previous restore point

Before making any significant changes to the system, it would be useful to complete some initial troubleshooting tasks that would not modify the system configuration. There's also no evidence that the current configuration is the root cause of this issue.

D. Perform a Windows Reset

A Windows Reset would be a significant change, and there's no evidence that the current Windows configuration is contributing to the slowdowns.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Solutions

<https://professormesser.link/1002030102>

**B65.** A network administrator is installing a set of upgraded Internet routers in the data center. Which of the following would be the best choices to secure the access to the data center door? (Select TWO)

- A.** Biometric lock
  - B.** USB lock
  - C.** Locking cabinet
  - D.** Privacy filter
  - E.** Cable lock
  - F.** Mantrap
- 

**The Answer:** **A.** Biometric lock and **F.** Mantrap

A biometric door lock provides access based on a fingerprint, handprint, or some other biometric characteristic. A mantrap is often used to limit or control the flow of people through a particular area. Often a mantrap is used in conjunction with additional authentication factors to allow or prevent access to an area.

**The incorrect answers:**

**B.** USB lock

A USB (Universal Serial Bus) lock is used to physically secure the USB interfaces on a computing device. USB locks are not used to secure access doors.

**C.** Locking cabinet

A locking cabinet is an important security feature on an equipment rack, but locking cabinets are not used to secure the doors to a data center.

**D.** Privacy filter

A privacy filter protects the contents of a screen from being seen by others. A privacy filter is not used to limit access to a data center door.

**E.** Cable lock

A cable lock is commonly used to securely fasten devices to a solid object to prevent theft. Cable locks are not used to secure access to data centers.



**More information:**

220-1002, Objective 2.1 - Physical Security

<https://professormesser.link/1002020101>

**B66.** An administrator is troubleshooting an error message that appears each time an application is started. The administrator has uninstalled and reinstalled the application, but the error message still appears. Which of the following would be the BEST next troubleshooting step?

- A. Use Performance Manager to monitor the system
  - B. Check the Event Viewer logs
  - C. View the hardware settings in Device Manager
  - D. Disable unneeded background processes in Services
- 

**The Answer:** B. Check the Event Viewer logs

The Windows Event Viewer can provide extensive information about the operating system and the applications. Error messages and application failures are logged in the Event Viewer for review.

**The incorrect answers:**

A. Use Performance Manager to monitor the system

Performance Manager provides long-term views of system metrics, such as CPU, memory, and network resource usage. Performance Manager is not used to monitor application failures.

C. View the hardware settings in Device Manager

The Device Manager can view and manage the hardware on a Windows computer. The Device Manager does not track application problems.

D. Disable unneeded background processes in Services

Although a Windows Service may be the root cause of this issue, we don't have enough information to make that determination. Instead of guessing at an issue, it would be a more directed and efficient process to gather information on the actual error using Windows Event Viewer.



#### More information:

220-1002, Objective 1.5 - Windows Administrative Tools

<https://professormesser.link/1002010501>

**B67.** Daniel, a user in the accounting department, has received an email asking for payment of an outstanding invoice and a link to a third-party payment site. The email contains purchase information that appears to be correct, but additional research shows that the invoice number is not valid. Which of the following would BEST describe this attack type?

- A. Spear phishing
  - B. Spoofing
  - C. Shoulder surfing
  - D. Man-in-the-middle
- 

**The Answer:** A. Spear phishing

A spear phishing attacker will focus their efforts on specific people or parts of the organization. An attacker that contacts the accounting department with an invoice and payment site details would be considered spear phishing.

**The incorrect answers:**

**B. Spoofing**

Spoofing is a method of impersonation that attempts to gain access by pretending to be someone else. This email was not making a direct attempt to disguise itself as another person or entity.

**C. Shoulder surfing**

An attacker using shoulder surfing will read the contents of a screen from another angle, such as over the shoulder. This email was not part of a shoulder surfing attack.

**D. Man-in-the-middle**

A man-in-the-middle attack involves a third-party that is able to view or modify the conversation between others without the knowledge of the original parties. This email was directly from the attacker and did not involve a third-party.



**More information:**

220-1002, Objective 2.5 - Social Engineering Attacks

<https://professormesser.link/1002020501>

**B68.** A user has dropped off their laptop at the repair desk. A message taped to the laptop states: "Doesn't work." Which of the following would be the BEST next step?

- A. Start the laptop and look for any issues
  - B. Call the customer and ask for more information
  - C. Replace the power adapter and try booting the laptop
  - D. Use a diagnostics boot CD to run hardware tests
- 

**The Answer:** B. Call the customer and ask for more information

A problem report of "Doesn't work" doesn't provide enough information to begin troubleshooting. A quick call to the customer will allow the technician to ask more specific questions and ultimately will resolve the laptop problem faster.

**The incorrect answers:**

A. Start the laptop and look for any issues

There's no way to know what part of the laptop is having problems, so blindly stumbling through possible issues would not be the most efficient way to troubleshoot this issue.

C. Replace the power adapter and try booting the laptop

There's no evidence that the laptop's power adapter is faulty. Replacing hardware without knowing more about the problem would not be the best next troubleshooting step.

D. Use a diagnostics boot CD to run hardware tests.

Many hardware diagnostics disks use bootable media, but there's no way to know if the reported issue was hardware-related. Taking time to run a hardware diagnostics test would not be the most efficient troubleshooting step.



**More information:**

220-1002, Objective 4.7 - Communication

<https://professormesser.link/1002040701>

**B69.** Which of these describes a free, open-source operating system?

- A. macOS
  - B. Linux
  - C. Windows
  - D. iOS
- 

**The Answer:** B. Linux

The Linux operating system has become popular through the development in the open source community and free distribution of the operating system software.

**The incorrect answers:**

A. macOS

The macOS operating system is an Apple product that is not available as open source. Although the price of macOS is minimal, it is still not a free operating system.

C. Windows

The Windows operating system is a closed-source product from Microsoft. Windows is not distributed as a free operating system.

D. iOS

Apple's iOS is their closed-source mobile operating system for smartphones and tablets. iOS is included with the mobile hardware provided by Apple.



**More information:**

220-1002, Objective 1.1 - Operating Systems Overview

<https://professormesser.link/1002010101>

**B70.** An IT manager would like to provide users with the option to recover daily versions of documents and spreadsheets. A user will have the option to roll back to any daily version in the last month. Which of the following would be the BEST way to implement this feature?

- A.** Create a file-level backup each day
  - B.** Maintain a monthly image level backup
  - C.** Store full backup tapes at an off-site facility
  - D.** Assign each user a USB flash drive
- 

**The Answer:** **A.** Create a file-level backup each day

Given the available options, the best way to create a separate version of every file each day will be to perform a file-level backup every 24 hours.

**The incorrect answers:**

**B.** Maintain a monthly image level backup

A monthly backup that images the entire computer does not provide a method to restore daily versions of a document.

**C.** Store full backup tapes at an off-site facility

Although daily full backups would provide a method of restoring document versions, maintaining those backups at an off-site facility would cause delays in the restoration of those documents.

**D.** Assign each user a USB flash drive

Requiring the users to maintain their own backup media would not be the best way to implement this requirement. A backup system requires centralized management and control of the backup media for both recovery and security purposes.



#### More information:

220-1002, Objective 4.3 - Disaster Recovery

<https://professormesser.link/1002040301>

**B71.** A network administrator has found that a daily report shows a single user with numerous visits to a website that violates the company's AUP. Which of the following should the administrator do NEXT?

- A. Create a firewall filter to block the website
  - B. Scan all computers with the latest anti-malware signatures
  - C. Contact the company's security officer
  - D. Change the user's password
- 

**The Answer:** C. Contact the company's security officer

A company's AUP (Acceptable Use Policy) is in place to limit the legal liability of an organization. If a person in the organization is not following the terms of the AUP, then the security officer's team should manage the results of that action.

**The incorrect answers:**

**A.** Create a firewall filter to block the website

A firewall filter may successfully prevent the user from visiting that site, but the original problem of the user browsing to the site still exists. This might be an eventual result of this situation, but it would not be the best next step.

**B.** Scan all computers with the latest anti-malware signatures

There's nothing in this particular situation that would indicate that the inappropriate website was a security risk or that the end user's computer was infected with malware.

**D.** Change the user's password

Locking out the user by changing their password might cause other issues that are outside the scope of the AUP violation. This also does not resolve the issue associated with the original website visits.



#### More information:

220-1002, Objective 4.1 - Documentation Best Practices

<https://professormesser.link/1002040101>

**B72.** Which of the following script extensions would commonly be used inside of a Microsoft Office application?

- A. .vbs
  - B. .py
  - C. .bat
  - D. .js
- 

**The Answer:** A. .vbs

The .vbs extension is used for Microsoft Visual Basic Scripting Edition scripts. These scripts provide general purpose scripting in Windows, and are especially common inside of Microsoft Office applications.

**The incorrect answers:**

**B. .py**

The .py extension is commonly used for the general-purpose scripting language of Python. Python is used on many operating systems, but it is not a common scripting language inside of Microsoft Office applications.

**C. .bat**

Scripts that run at the Windows command line are batch files that use the .bat extension. These batch files are not commonly used in Microsoft Office applications.

**D. .js**

Scripts that run inside of a browser commonly use JavaScript files with the .js extension. JavaScript is not the most common scripting language for Microsoft Office applications.



**More information:**

220-1002, Objective 4.8 - Scripting

<https://professormesser.link/1002040801>

- B73.** A system administrator has installed a SOHO network of five Windows computers. The administrator would like to provide a method of sharing documents and spreadsheets between all of the office computers. Which of the following would be the BEST way to provide this functionality?
- A.** Domain
  - B.** Proxy server
  - C.** Workgroup
  - D.** Remote Desktop
- 

**The Answer:** **C.** Workgroup

A Windows Workgroup is a common data sharing methods for small departments that maintain documents on their own computers.

**The incorrect answers:**

**A.** Domain

Microsoft's Active Directory Domain Services are designed for larger organizations that need centralized management of user accounts, computing devices, and servers.

**B.** Proxy server

A proxy server is used to secure and control network communication. A proxy server is not used for sharing documents in an office.

**D.** Remote Desktop

The Remote Desktop feature in Windows allows a device to view and control the screen of another computer. Remote Desktop functionality is not used for sharing files.



**More information:**



220-1002, Objective 1.8



HomeGroups, Workgroups, and Domains

<https://professormesser.link/1002010801>

**B74.** A user took pictures of a new company product on their Apple tablet. Those pictures were posted on an industry rumor website the following week. Which of the following should be evaluated as the MOST likely security concern?

- A. iCloud
  - B. OneDrive
  - C. Google Sync
  - D. iTunes
- 

**The Answer:** A. iCloud

Apple's iCloud is the cloud-based service that provides an online backup for iOS devices. If an attacker gains access to an iCloud account, they will be able to access photos, notes, and other information from the iOS device.

**The incorrect answers:**

**B. OneDrive**

OneDrive is Microsoft's cloud-based service for Windows computers. Windows devices will store files, configurations, and other documents in the OneDrive cloud.

**C. Google Sync**

Android devices use Google Sync to maintain a backup of an Android phone or tablet.

**D. iTunes**

iTunes is software that runs on a local computer to manage and backup Apple iOS devices. iTunes files are stored on local devices, making them relatively more secure than files stored in the cloud.



**More information:**

220-1002, Objective 3.5

Troubleshooting Mobile Device Security

<https://professormesser.link/1002030501>

**B75.** A manufacturing company in the United States provides monthly subscriptions and is storing customer credit card information for these recurring charges. Which of the following would be the MOST important set of policies to follow?

- A.** GDPR
  - B.** PCI DSS
  - C.** EULA
  - D.** PHI
- 

**The Answer:** **B.** PCI DSS

The PCI DSS (Payment Card Industry Data Security Standard) is a set of objectives designed to secure credit cards and financial transactions. Companies storing credit card information must comply with these standards to accept credit cards for payment.

**The incorrect answers:**

**A. GDPR**

GDPR (General Data Protection Regulation) is a set of data protection and privacy laws for individuals in the European Union. The GDPR is not associated with credit card transactions in the United States.

**C. EULA**

A EULA (End User Licensing Agreement) determines how software can be used. The EULA is provided by the software manufacturer and is followed by the users of the software.

**D. PHI**

PHI (Protected Health Information) in the United States is governed by the Health Insurance Portability and Accountability Act of 1996, or HIPAA. PHI data is not associated with credit card transactions.



**More information:**

220-1002, Objective 4.6 - Privacy, Licensing, and Policies  
<https://professormesser.link/1002040601>

**B76.** A user is traveling to a conference and they would like to be sure that any messages sent from their phone during the event remain private while using the event's wireless hotspot. Which of the following should be configured on this user's phone?

- A.** VPN
  - B.** Strong password
  - C.** Network-based firewall
  - D.** Multi-factor authentication
- 

**The Answer:** **A.** VPN

A VPN (Virtual Private Network) would allow a remote user to connect to the corporate office over a secure encrypted tunnel.

**The incorrect answers:**

**B.** Strong password

A strong password would prevent someone from accessing or authenticating to the user's phone, but it would not protect the privacy of messages sent from the phone.

**C.** Network-based firewall

A network-based firewall must be connected to the network to be effective. Network-based firewalls are not configured on a phone.

**D.** Multi-factor authentication

Multi-factor authentication adds additional login parameters, but it doesn't change the type of traffic sent over the network.



**More information:**

220-1002, Objective 2.2 - Logical Security

<https://professormesser.link/1002020201>

**B77.** A company is installing a new wireless access point in a conference room. Which of the following would provide the BEST security for this network?

- A.** RC4
  - B.** WPA2
  - C.** TKIP
  - D.** WEP
- 

**The Answer:** **B.** WPA2

WPA2 (Wi-Fi Protected Access version 2) provides the best security among all of the available options. The WPA2 standard is a very common security standard for wireless networks.

**The incorrect answers:**

**A. RC4**

RC4 (Rivest Cipher 4) is an encryption method used on the original version of WPA. The cryptographic technologies used in WPA2 are considered to be more secure than those used in WPA.

**C. TKIP**

TKIP (Temporal Key Integrity Protocol) provides integrity checks and prevents replay attacks in the original WPA protocol. TKIP has some known vulnerabilities, so WPA would not be the most secure option for this network.

**D. WEP**

WEP (Wired Equivalent Privacy) was one of the original wireless encryption standards. WEP was found to have significant cryptographic vulnerabilities, so it would not be a secure option for any network.



**More information:**

220-1002, Objective 2.3 - Wireless Security

<https://professormesser.link/1002020301>

**B78.** A server administrator has configured an automated process to backup VM snapshots each evening during non-working hours. The backups will be stored on a series of high-density tape drives. How can the administrator confirm that these backups will be useful when a server recovery is needed?

- A. Send the backups to an off-site facility
  - B. Connect the tape drives to a UPS
  - C. Create separate file-level backups
  - D. Perform occasional recovery tests
- 

**The Answer:** D. Perform occasional recovery tests

The best way to confirm that a backup will be useful when needed is to perform occasional audits of the existing backup media. This is an important step that should be followed for all backup processes.

**The incorrect answers:**

A. Send the backups to an off-site facility

Sending the backups to an off-site location may help protect the data and preserve the information over a longer timeframe, but it doesn't improve the quality of data stored on the tapes.

B. Connect the tape drives to a UPS

Most of the infrastructure equipment in a data center should be connected to a UPS (Uninterruptible Power Supply), but having that reliable power connection doesn't guarantee that the data stored on the tapes will be valid during the restore process.

C. Create separate file-level backups

Creating additional backups is a good best practice, but having separate backup files doesn't change the quality of the data stored on the original backup tapes.



**More information:**

220-1002, Objective 4.3 - Disaster Recovery

<https://professormesser.link/1002040301>

- B79.** A system administrator needs to configure a laptop to support inbound Remote Desktop services for the help desk team. Which of these Control Panel applets provides access to these settings?
- A.** Internet Properties
  - B.** Devices and Printers
  - C.** Network and Sharing Center
  - D.** System
- 

**The Answer:** **D.** System

The System applet includes a Remote tab for Remote Assistance and Remote Desktop. The Remote Desktop option is available in non-Home editions of Windows.

**The incorrect answers:**

**A.** Internet Properties

The Internet Properties applet includes configuration options for the browser and configuration settings for proxies.

**B.** Devices and Printers

The Devices and Printers applet allows for the addition, removal, or configuration of monitors, storage drivers, printers, and more.

**C.** Network and Sharing Center

The Network and Sharing Center provides access to network configurations, file sharing options, and other network-related configurations. The options for Remote Desktop are not located in the Network and Sharing Center.



**More information:**

220-1002, Objective 1.8 - Windows Network Technologies  
<https://professormesser.link/1002010802>

**B80.** A user has dropped off a laptop to the help desk and states that the laptop is experiencing a problem during the boot process. Which of these options would be the best path to resolve this issue?

- A. When the customer provides enough information, stop them and let them know when they can pick up the laptop
  - B. Take the laptop and tell the customer to return tomorrow
  - C. Repeat an understanding of the issue back to the customer for verification
  - D. Provide recommendations to the customer with proper technical IT explanations
- 

**The Answer:** C. Repeat an understanding of the issue back to the customer for verification

It's important to communicate with the client to determine the issue and to verify with the customer that the technician has properly documented the problem.

**The incorrect answers:**

A. When the customer provides enough information, stop them and let them know when they can pick up the laptop

It would be inappropriate to interrupt the customer before the complete issue is communicated to the technician. It's very possible that some important information will be missed without getting a full report from the customer.

B. Take the laptop and tell the customer to return tomorrow

Without understanding the issue, it's impossible to know if the problem can be resolved in 24 hours.

D. Provide recommendations to the customer with proper technical IT explanations

The customer may not be an information technology professional, so using technical jargon is not going to be an effective way to communicate with the customer.



**More information:**

220-1002, Objective 4.7 - Communication

<https://professormesser.link/1002040701>

**B81.** A technician is upgrading the motherboard in a server. Which of the following should be the FIRST task when beginning this upgrade?

- A.** Wear safety goggles
  - B.** Connect an ESD strap
  - C.** Remove any motherboard batteries
  - D.** Disconnect from all power sources
- 

**The Answer:** **D.** Disconnect from all power sources

When working inside of a computer, it's always important to disconnect the system from the main power source. This should always be the first and most important step when working on the inside of a device.

**The incorrect answers:**

**A.** Wear safety goggles

Safety goggles aren't commonly required when working inside of a computer case. Goggles would only be required if extensive dust or debris was a concern, and it would not be needed until the power source was disconnected.

**B.** Connect an ESD strap

An ESD (Electrostatic Discharge) strap should be used to minimize the chance of damage from static electricity. This strap should not be attached until the main power source was disconnected.

**C.** Remove any motherboard batteries

It's not necessary to remove the batteries on a motherboard during a replacement. If the new motherboard does not have a battery, then the battery can be moved between systems.



**More information:**

220-1002, Objective 4.4 - Safety Procedures

<https://professormesser.link/1002040401>

**B82.** A system administrator is installing a new video editing application on a user's workstation from an installation DVD-ROM. However, the installation process fails due to lack of available drive space. Which of the following would be the BEST way to complete the installation process?

- A.** Use a USB drive for the installation source
  - B.** Compress the installation files
  - C.** Install the application to a network share
  - D.** Manually copy the installation files to the application directory
- 

**The Answer:** **C.** Install the application to a network share

The installed application files can be much larger than the installation utility, so using a network share with a larger available storage space can be a good alternative until free space is available on the local computer.

**The incorrect answers:**

**A.** Use a USB drive for the installation source

Changing the installation media from a DVD-ROM (Digital Versatile Disc - Read Only Memory) to a USB (Universal Serial Bus) drive would not provide any additional free space on the destination storage drive.

**B.** Compress the installation files

Most installation files are already compressed, but compressing files on the installation media would not provide additional free space on the application storage drive.

**D.** Manually copy the installation files to the application directory

Most installation programs do not simply copy the existing files to a directory. The installation program often uncompresses the files, updates registry settings, and updates Windows configurations. Manually copying the files would not result in a properly installed application, and it would not provide any additional free space for the installation.



#### More information:

220-1002, Objective 1.7 - Installing Applications  
<https://professormesser.link/1002010701>

**B83.** A user would like to install an image and photo editing program on their home computer, but they would prefer an application that did not require a monthly subscription. Which of the following would be the BEST licensing option for this requirement?

- A.** FOSS
  - B.** Enterprise
  - C.** Personal
  - D.** Site
- 

**The Answer:** **A.** FOSS

FOSS (Free and Open-Source) software is distributed without charge and includes a copy of the source code.

**The incorrect answers:**

**B.** Enterprise

Software using an enterprise license is designed for large-scale deployments and commonly requires a per-seat or per-use cost.

**C.** Personal

A personal license is often purchased individually, but there is still a cost for the license.

**D.** Site

Site licenses are often used by large organizations to purchase licenses for all of their devices.



**More information:**

220-1002, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1002040601>

**B84.** A system administrator is troubleshooting an issue with an application. The application uses an increasing amount of memory until all available RAM is eventually depleted. The computer must be rebooted every few days when this memory issue occurs. Which of the following utilities would show how much RAM is used by this application?

- A. Event Viewer
  - B. Device Manager
  - C. Task Manager
  - D. Programs and Features
- 

**The Answer: C. Task Manager**

Task Manager provides a real-time view of system metrics, including CPU utilization, storage use, and memory utilization.

**The incorrect answers:**

**A. Event Viewer**

The Windows Event Viewer is a consolidated log of all system events. Real-time memory usage is not monitored by the Event Viewer.

**B. Device Manager**

The Device Manager provides management of the hardware device drivers. Resource utilization and memory information is not provided in Device Manager.

**D. Programs and Features**

Applications and Windows features can be installed or removed from the Programs and Features applet. Programs and Features does not display memory utilization statistics.



**More information:**

220-1002, Objective 1.5 - Task Manager

<https://professormesser.link/1002010504>

- B85.** An administrator is troubleshooting a desktop computer that is experiencing a reboot loop. Before the Windows login screen appears, the system reboots in a continuous loop. Which of the following would be the BEST way to address this issue?
- A. Start Safe Mode and perform a defragmentation
  - B. Reinstall the operating system from the original media
  - C. Update the boot order from the system BIOS
  - D. Run Startup Repair from the Advanced Boot Options
- 

**The Answer:** D. Run Startup Repair from the Advanced Boot Options

The Windows Startup Repair can resolve many problems with the startup process, including problems with drivers that are failing and resetting during boot.

**The incorrect answers:**

A. Start Safe Mode and perform a defragmentation

There's no guarantee that Safe Mode would start normally on this system. If it did provide access to the Windows desktop, running a defragmentation would not solve the rebooting loop.

B. Reinstall the operating system from the original media

Before making a significant change to the operating system and configuration of the computer, it's worthwhile to run through some repair options.

C. Update the boot order from the system BIOS

The rebooting loop is not related to the boot order, and making changes to the boot order would not resolve any issues that are causing the looping to occur.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Solutions

<https://professormesser.link/1002030102>

**B86.** A user has downloaded a browser add-on that assists with new car purchases. During the installation, the Windows UAC is requesting administrative permissions to continue with the install. Which of these is the MOST likely situation?

- A. The operating system requires an update
  - B. The software is a Trojan horse
  - C. The workstation is already part of a botnet
  - D. A worm will be downloaded and installed
- 

**The Answer:** B. The software is a Trojan horse

A UAC (User Account Control) prompt is a security feature that asks for additional permissions when an application wants to make unauthorized changes to the operating system. If a relatively simple application is causing the UAC message to appear, then it may be a Trojan horse trying to install itself by pretending to be something else.

**The incorrect answers:**

A. The operating system requires an update

The UAC prompts are not associated with the OS update process. The Windows Update will download and install operating system updates behind the scenes without requiring displaying any UAC messages.

C. The workstation is already part of a botnet

A workstation that is already part of a botnet would not cause a UAC prompt to appear during the installation of a browser add-on.

D. A worm will be downloaded and installed

The UAC prompt occurs when the application needs access that the user does not normally have. It's not possible to know what would be downloaded and installed until it actually occurs.



**More information:**

220-1002, Objective 2.4 - Types of Malware

<https://professormesser.link/1002020401>

**B87.** An organization has distributed new laptops to all of their home-office employees. Although the users at home can successfully connect through the Internet to resources at the corporate office, there have been complaints that printers and shared drives at home are not accessible. Which of the following would explain this issue?

- A. Incorrect login credentials
  - B. Port security is turned on
  - C. The corporate VPN is enabled
  - D. Blocked by DLP
- 

**The Answer:** C. The corporate VPN is enabled

A VPN (Virtual Private Network) connection that sends all traffic back to the corporate office by default would effectively disconnect the user from any other local resources, such as printers, other computers, and local file shares.

**The incorrect answers:**

**A. Incorrect login credentials**

Incorrect login credentials would prevent access to all resources, including those at the corporate office over the VPN.

**B. Port security is turned on**

Port security is a feature configured on a switch interface to prevent an unauthorized user from physically connecting to a switch. Port security would limit all traffic through the network, including the traffic intended for the corporate office.

**D. Blocked by DLP**

DLP (Data Loss Prevention) is a security technology that will identify and block the transfer of unauthorized materials through the network. DLP solutions are often used to block private customer information, credit card details, and other sensitive data. A DLP solution would not be the reason that communication to home resources would be blocked.



**More information:**

220-1002, Objective 2.2 - Logical Security

<https://professormesser.link/1002020201>

**B88.** A user on the marketing team is experiencing slower load times and ongoing sluggishness with applications on their laptop. A technician examines the Windows Update logs and finds that the monthly updates are failing. Which of the following should be the best NEXT step for resolving this issue?

- A.** Perform an anti-malware scan
  - B.** Install the Windows Updates manually
  - C.** Increase the amount of RAM in the laptop
  - D.** Re-install the applications
- 

**The Answer:** **A.** Perform an anti-malware scan

The combination of slower applications, poor load times, and the failure of Windows updates, indicates that the system may be infected with malware. Given the available options, an anti-malware scan would be the best next troubleshooting step.

**The incorrect answers:**

**B.** Install the Windows Updates manually

There's no evidence that a lack of Windows Updates is causing application sluggishness and slow load times. Before making any significant operating system changes, it would be useful to run some initial scans and tests.

**C.** Increase the amount of RAM in the laptop

The laptop used to perform well, which indicates that the amount of RAM in the system was sufficient. Before going through the time and expense of an upgrade, it would be worthwhile to know the root cause of the slowdowns.

**D.** Re-install the applications

It would be unusual for all applications to have problems at the same time, so reinstalling the application would most likely not resolve any issues. Before making changes, a bit more research would be called for.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues

<https://professormesser.link/1002030201>

**B89.** A desktop administrator is troubleshooting an error that randomly causes a workstation to spike to 100% utilization. Which of these utilities would help the administrator track and report on system utilization over a 24-hour period?

- A.** Performance Monitor
  - B.** Device Manager
  - C.** Services
  - D.** Task Scheduler
- 

**The Answer:** **A.** Performance Monitor

The Windows Performance Monitor can track and store long-term information on many different system resources, including CPU, memory, network performance, and more.

**The incorrect answers:**

**B.** Device Manager

The Device Manager is the central management utility for hardware device drivers. Device Manager does not provide a way to track system utilization over time.

**C.** Services

The Services applet will allow the administrator to view and control the background services on a Windows computer. The Services utility will not display system utilization over time.

**D.** Task Scheduler

The Windows Task Scheduler will run scripts and applications on certain dates and times. Task Scheduler does not gather performance metrics.



**More information:**

220-1002, Objective 1.5 - Windows Administrative Tools  
<https://professormesser.link/1002010501>

**B90.** Which of these would be the BEST way to prevent an attacker from modifying default routes on a SOHO wireless network?

- A. Configure MAC address filtering
  - B. Enable WPS connectivity
  - C. Change the router's default password
  - D. Disable unneeded interfaces
- 

**The Answer:** C. Change the router's default password

The login credentials to a SOHO (Small Office / Home Office) router protect the device from configuration changes. If the default password is configured on a router, then anyone would be able to make changes on the device.

**The incorrect answers:**

**A.** Configure MAC address filtering

MAC (Media Access Control) address filtering is an administrative tool that can allow or deny access to the network. MAC filtering is not a security feature.

**B.** Enable WPS connectivity

WPS (Wi-Fi Protected Setup) is a configuration method for securely connecting devices to a wireless network. WPS is not used to protect the configuration settings of a router.

**D.** Disable unneeded interfaces

Limiting access to interfaces is a good best practice, but it doesn't prevent an attacker from changing the configurations in the router.



**More information:**

220-1002, Objective 2.10 - Securing a SOHO Network  
<https://professormesser.link/1002021001>

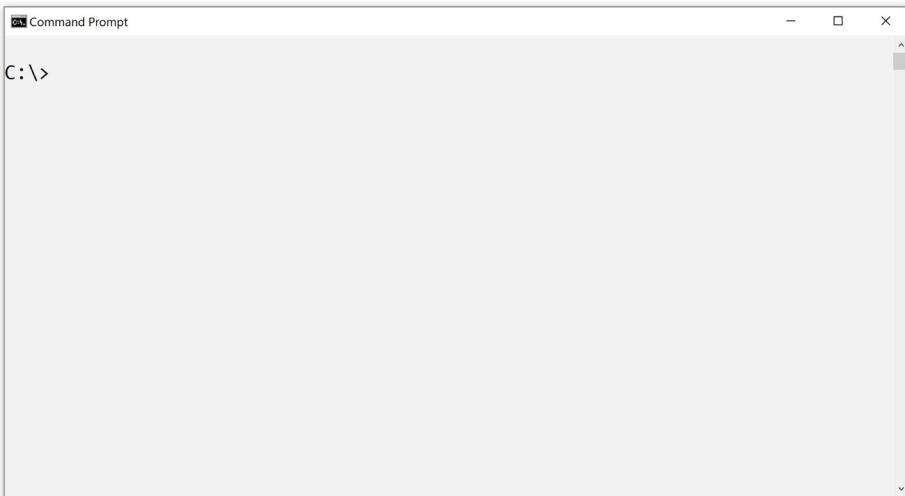




# Practice Exam C

## Performance-Based Questions

- C1. A Windows desktop administrator would like to query the local DNS server to view the IP address and for www.professormesser.com. Use a command line utility to view this information.



```
Command Prompt

C:\>
```

**C2.** Match the Linux command to the description.

Some descriptions will not have a match.

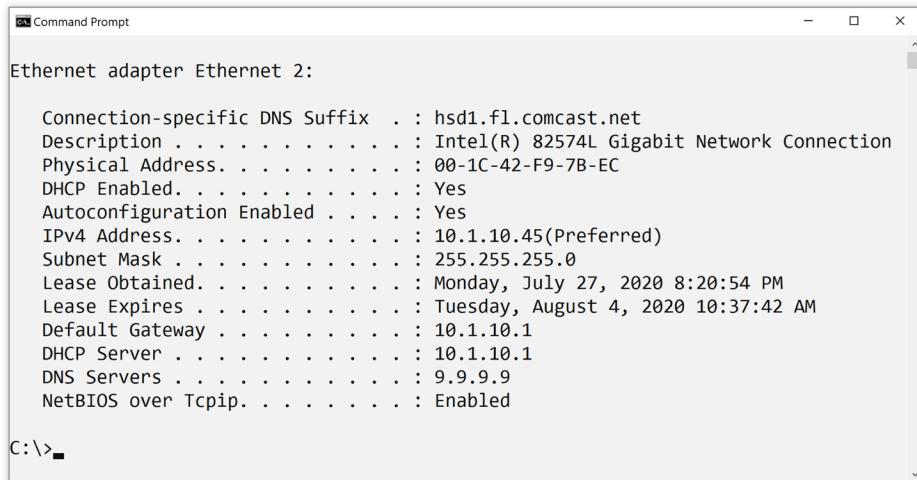
**Commands:**

mv
pwd
chmod
grep

**Descriptions:**

Display the current working directory path
Run a program with elevated permissions
Modify the owner of a file
Change a user's password
Rename a directory
Search through files for the word "transaction"
Make a file read-only

**C3.** A user has contacted the help desk because they are not able to browse any websites. What command line utility would be able to confirm the connectivity to a server that could convert fully qualified domain names to IP addresses?

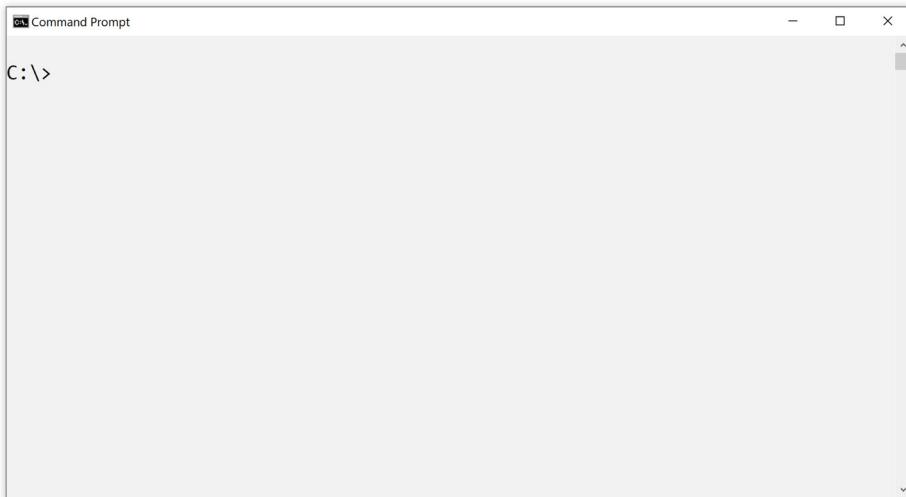


```
Command Prompt
Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : hsd1.fl.comcast.net
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-1C-42-F9-7B-EC
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 10.1.10.45(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, July 27, 2020 8:20:54 PM
Lease Expires . . . . . : Tuesday, August 4, 2020 10:37:42 AM
Default Gateway . . . . . : 10.1.10.1
DHCP Server . . . . . : 10.1.10.1
DNS Servers . . . . . : 9.9.9.9
NetBIOS over Tcpip. . . . . : Enabled

C:\>
```

- C4.** An application, foothold.exe, has become unresponsive and the user is not able to close the application normally from the Windows desktop. Use the Windows command line to terminate this application.



- 
- C5.** Match the Control Panel applet to the description.

Some descriptions will not have a match.

**Applets:**

**Descriptions:**

User Accounts	Protect all data saved on a volume
File Explorer Options	Disable a USB audio controller
Credential Manager	Disable indexing of system directories
Device Manager	View website certificates
	Update a spreadsheet when away from the office
	Change an account to an Administrator
	Save a website username and password

---



# Practice Exam C

## Multiple Choice Questions

**C6.** A technician has been called to resolve an issue with a desktop computer in a training facility. The computer appears to boot properly to the desktop, but applications take five minutes to load. While using the application, pop-up messages and other windows appear on the desktop. Which of the following should be the best NEXT troubleshooting step?

- A.** View running processes in Task Manager
- B.** Disable System Restore
- C.** Remove the computer from the network
- D.** Educate the end user

Quick  
Answer: **291**

The Details: **298**

**C7.** A system administrator would like to disable the TFTP Client in Windows 10. Which of the following Control Panel applets would be the BEST choice for this task?

- A.** Programs and Features
- B.** Services
- C.** Credential Manager
- D.** File Explorer options

Quick  
Answer: **291**

The Details: **299**

**C8.** A user has noticed that a Bluetooth device is currently connected to their tablet, but they don't recognize the make or model of the connected device. Which of the following would be the FIRST step for troubleshooting this issue?

- A.** Perform an anti-malware scan
- B.** Research installed apps with an app scanner
- C.** Disable the Wi-Fi network
- D.** Remove the Bluetooth device

Quick  
Answer: **291**

The Details: **300**

**C9.** A user has recently been assigned a new tablet, but each time she tries to read email messages she receives the message, “The email could not be decrypted.” The user has reinstalled the email client, but the problem still occurs over both Internet and VPN connections. Which of the following would be the best way for a technician to resolve this issue?

- A.** Ask the user to reset their password
- B.** Change the user's email alias
- C.** Send the user a certificate with a private key
- D.** Confirm the wireless network encryption settings

Quick  
Answer: **291**

The Details: **301**

**C10.** A computer technician has been asked to verify a set of new Group Policy settings on computers at a remote site. Which of the following commands should be used to validate the last policy update on the systems?

- A.** net view
- B.** sfc
- C.** gpresult
- D.** netstat
- E.** dism

Quick  
Answer: **291**

The Details: **302**

**C11.** A system administrator needs to modify the Linux group associated with a file. Which of the following would provide this functionality?

- A.** ps
- B.** ifconfig
- C.** chown
- D.** grep

Quick  
Answer: **291**

The Details: **303**

**C12.** A user has brought their laptop to the help desk because of an issue during startup. The laptop screen remains black when powering on, and no status lights appear on the system. The user is traveling tomorrow to a remote site in another country and needs the laptop while they are on the road. Which of the following would be the best NEXT choice?

- A.** Provide the user with the option to repair, replace, or rent a new system
- B.** Assign the user to the standard seven-day repair agreement
- C.** Replace the external power cable and close the repair ticket
- D.** Recommend the user cancel their travel plans

Quick  
Answer: **291**

The Details: **304**

**C13.** A home user provides numerous online presentations during the day, but the power in their area is not stable and there will often be short power outages. Which of the following would help with this issue?

- A.** Cloud backups
- B.** External storage device
- C.** UPS
- D.** Surge suppressor

Quick  
Answer: **291**

The Details: **305**

**C14.** A system administrator is planning to upgrade two physical servers in the corporate data center to external cloud-based platforms. Which of the following would provide information on connectivity and the plans for remote site access?

- A.** Change scope
- B.** End-user acceptance
- C.** Backout plan
- D.** Risk analysis

Quick  
Answer: **291**

The Details: **306**

**C15.** A system administrator would like to conserve bandwidth to remote sites connected over slower network links. Which of these Windows features would provide this functionality?

- A.** EFS
- B.** Domain Services
- C.** BitLocker
- D.** BranchCache

Quick  
Answer: **291**

The Details: **307**

**C16.** A user has just installed a driver update from a laptop manufacturer. After restarting, their system shows a Windows Stop Error before the login prompt is displayed. Each subsequent reboot causes the same error to be displayed. Which of the following should the system administrator follow to BEST resolve this issue?

- A.** Modify the BIOS boot order
- B.** Boot to Safe Mode and perform a Windows Reset
- C.** Perform a System Restore
- D.** Reinstall the patch files

Quick  
Answer: **291**

The Details: **308**

**C17.** The available storage space on a user's workstation is running low, and some updates are failing due to insufficient drive space. Which of the following would be the BEST way to increase drive space until a larger storage drive can be installed?

- A.** Use a Guest login
- B.** Enable System Protection
- C.** Disable Remote Assistance
- D.** Set the paging file size to zero

Quick  
Answer: **291**

The Details: **309**

**C18.** A technician is troubleshooting a Windows 10 computer that is performing very slowly when moving from one application to another. Which of the following utilities would allow the technician to view real-time resource activity?

- A.** Services
- B.** Task Manager
- C.** System Information
- D.** Device Manager

Quick  
Answer: **291**

The Details: **310**

**C19.** An attacker has gained access to a password hash file. Which of the following will the attacker use to obtain the passwords?

- A. DoS
- B. Decryption
- C. Brute force
- D. Phishing

Quick  
Answer: 291

The Details: 311

**C20.** A server administrator needs to create a folder on a Windows server to store weekly status report documents. Which of the following command-line tools would provide this functionality?

- A. mkdir
- B. net use
- C. cd
- D. dir
- E. ls

Quick  
Answer: 291

The Details: 312

**C21.** A desktop administrator is troubleshooting a laptop computer experiencing slowdowns and delays during normal operation. There are many icons displayed at the bottom of the Windows desktop, and an error message on the screen shows “Out of memory or system resources.” Which of the following troubleshooting steps would be the BEST way to address this issue?

- A. Use Task Manager to close applications
- B. Reboot the computer
- C. Release and renew the network connection
- D. Roll back to a previous restore point

Quick  
Answer: 291

The Details: 313

**C22.** A desktop administrator is removing a virus from a laptop computer in a shared lab. The computer has been removed from the network and the System Restore feature has been disabled. When the administrator attempts to update to the latest anti-virus signatures, the anti-virus utility disables itself. Which of the following would be the best NEXT step?

- A.** Boot to Safe Mode and use signatures downloaded from a separate computer Quick  
Answer: 291
- B.** Roll back to a previous configuration The Details: 314
- C.** Schedule periodic updates and reconnect to the network
- D.** Discuss anti-virus strategies with the end user

**C23.** A Windows 10 computer is displaying a series of error messages during the startup process. A technician has been dispatched and would like to view more information about the errors without restarting the computer. Which of the following utilities would provide the technician with more details about these messages?

- A.** taskschd Quick
- B.** devmgmt Answer: 291
- C.** perfmon The Details: 315
- D.** eventvwr
- E.** sfc

**C24.** A user's corporate smartphone has stopped responding to screen touches or button presses. Which of the following would be the BEST way to resolve this issue?

- A.** Connect the smartphone to a power source Quick
- B.** Perform a hard reset Answer: 291
- C.** Reset the Internet router The Details: 316
- D.** Power off all Bluetooth devices

**C25.** Jack, a technician, has been asked to replace a faulty adapter card in a server. Jack does not have an anti-static strap to use for this repair, but he has removed the server from a power source. Which of the following would be the BEST way to safely complete this repair?

- A. Store the faulty card in an anti-static bag
- B. Periodically touch the server's metal chassis
- C. Wear safety goggles
- D. Have a carbon dioxide extinguisher nearby

Quick  
Answer: **291**

The Details: **317**

**C26.** Which of the following would be the BEST choice for a system administrator to manage an Active Directory database?

- A. Batch file
- B. PowerShell
- C. JavaScript
- D. Visual Basic Scripting

Quick  
Answer: **291**

The Details: **318**

**C27.** Jack, a user, has started his computer and received this message on the screen:

“Your important files are encrypted. If you want to decrypt all of your files, you need to pay.”

Sam, a desktop administrator, has confirmed that Jack can no longer access his desktop, and none of his installed applications are available in the system menus. Sam notices that a payment link is posted at the bottom of the screen. Which of the following would BEST describe this scenario?

- A. Spyware
- B. Boot sector virus
- C. Rootkit
- D. Crypto-malware

Quick  
Answer: **291**

The Details: **319**

**C28.** A desktop technician has received a complaint that a remotely-hosted application has stopped working. The technician believes that a network outage at the application provider is the root cause of the issue. Which of the following tools would be the BEST choice to confirm the location of the outage?

- A.** ping
- B.** nslookup
- C.** netstat
- D.** traceroute

Quick  
Answer: **291**

The Details: **320**

**C29.** Users on the corporate network authenticate once at the beginning of the day, and are not prompted again for authentication until the following day. Which of the following would BEST describe this functionality?

- A.** NTFS
- B.** SSO
- C.** Inherited permissions
- D.** EFS

Quick  
Answer: **291**

The Details: **321**

**C30.** A server technician is removing the memory from a web server and adding new memory modules to the motherboard. The old memory modules will be used to upgrade a server in a different data center. Which of the following would be the BEST way to protect the old memory modules?

- A.** Padded envelope
- B.** Cotton fabric
- C.** Molded foam packing material
- D.** Anti-static bag

Quick  
Answer: **291**

The Details: **322**

**C31.** A Linux administrator is using the grep command while monitoring a database application. Which of the following would BEST describe this activity?

- A.** Search through a file for specific text
- B.** View a list of running processes
- C.** Change the permissions of a file
- D.** View the name of the working directory

Quick  
Answer: **291**

The Details: **323**

**C32.** A Windows 10 application includes the installation of a service during the setup process. Which of the following would be the MOST important consideration during the application setup?

- A.** OS compatibility
- B.** Available storage space
- C.** Network connectivity
- D.** User permissions

Quick  
Answer: **291**

The Details: **324**

**C33.** A medical center requires that shared computer systems are installed in hallways and patient rooms for the hospital staff. However, hospital administrators are concerned that patient information might be visible if someone leaves the computer without logging out. Which of the following would help prevent this type of issue?

- A.** Multi-factor authentication
- B.** Password expiration policy
- C.** Login time restrictions
- D.** Screensaver passwords

Quick  
Answer: **291**

The Details: **325**

**C34.** George, a user, has a smartphone to assist with maps and directions when traveling to other company locations. At a remote site, George finds that his phone is attempting to contact a third-party website to share location information. Which of the following would be the BEST way to address this issue?

- A.** Disable the GPS
- B.** Perform a soft reset
- C.** Run an anti-malware scan
- D.** Use the cellular network instead of Wi-Fi

Quick  
Answer: **291**

The Details: **326**

**C35.** A company requires all users to authenticate to a proxy before communicating to external websites. Which of the following should be used to integrate the proxy authentication with the existing Active Directory credentials?

- A.** WPS
- B.** TKIP
- C.** RADIUS
- D.** WPA2

Quick  
Answer: **291**

The Details: **327**

**C36.** A desktop administrator has been tasked with removing malware from an executive's laptop computer. The system has been removed from the network, but the Windows startup process shows a Stop Error before rebooting into a repeating cycle. Which of the following would be the best NEXT step in the malware removal process?

- A.** Perform a Windows Repair installation
- B.** Boot with a pre-installation environment
- C.** Schedule periodic scans
- D.** Create a restore point

Quick  
Answer: **291**

The Details: **328**

**C37.** An audit has found that numerous email attachments include non-encrypted documents containing credit card numbers. A security administrator has been asked to prevent this information from being sent across the network. Which of the following would be the BEST way to provide this functionality?

- A.** Enable Windows Firewall
- B.** Block all email at the Internet firewall
- C.** Create a Group Policy
- D.** Use a DLP solution
- E.** Require multi-factor authentication

Quick  
Answer: **291**

The Details: **329**

**C38.** A user has just upgraded a Windows application and has restarted their computer. Unfortunately, the Windows desktop no longer appears after the login process. Which of the following utilities would allow the system administrator to resolve this issue?

- A.** System Restore
- B.** Performance Monitor
- C.** bootrec
- D.** Task Manager
- E.** dxdiag

Quick  
Answer: **291**

The Details: **330**

**C39.** A user in the shipping department is using a tracking app on a tablet. The app normally takes 10 seconds to load, but is now taking over a minute before it can be used. Tracking searches that normally take seconds are taking almost a minute to show the tracking details. Other tablets are not experiencing this slowdown. Which of the following would be the best NEXT troubleshooting step?

- A.** Reinstall the tracking app
- B.** Check the app battery usage
- C.** Roll back to the previous tablet OS version
- D.** Perform a soft reset

Quick  
Answer: **291**

The Details: **331**

**C40.** Which of the following fire extinguishers would be most appropriate to use in a data center?

- A.** Foam
- B.** Carbon Dioxide
- C.** Saline
- D.** Water

Quick  
Answer: **291**

The Details: **332**

**C41.** The Human Resources department is installing a shared computer in the company lobby to use for electronic job applications. The kiosk should start automatically without requiring any network login prompt, and the kiosk should only have access to the job application modules. Which of the following account types would be the BEST choice for this system?

- A. SSO user
- B. Administrator
- C. Guest
- D. Power User

Quick  
Answer: **291**

The Details: **333**

**C42.** An administrator needs to configure a COM+ application on the company's workstations. Which of the following should be used to complete this task?

- A. Device Manager
- B. Local Security Policy
- C. Component Services
- D. Performance Monitor

Quick  
Answer: **291**

The Details: **334**

**C43.** A user in the shipping department is able to view order information, but they cannot modify or delete any order details. Which of the following would best describe this security principle?

- A. Multi-factor authentication
- B. Least privilege
- C. Group Policy
- D. Data loss prevention

Quick  
Answer: **291**

The Details: **335**

**C44.** A user has just completed the installation of a new video driver on their Windows 10 laptop and has rebooted the system. Instead of the Windows login screen, the laptop shows a black screen with no additional information or messages. Which of the following would be the best NEXT troubleshooting step?

- A. Update the BIOS
- B. Modify the BCD settings
- C. Start in VGA mode
- D. Update to the latest OS patches

Quick  
Answer: **291**

The Details: **336**

**C45.** A small office is located in a large office building that contains over fifty different companies. A network administrator would like to limit the possibility of someone else in the building accidentally connecting to their wireless network. Which of these configuration settings would prevent their wireless network from appearing in a list of available networks?

- A.** MAC filtering
- B.** Static IP addressing
- C.** WPA2 encryption
- D.** SSID suppression

Quick  
Answer: **291**

The Details: **337**

**C46.** A manager in the accounting department would like to upgrade to Windows 10, but she doesn't want to lose access to any of the currently installed applications or data. Which of the following methods would be the BEST choice for these requirements?

- A.** Clean install
- B.** Unattended installation
- C.** Network installation
- D.** In-place upgrade

Quick  
Answer: **291**

The Details: **338**

**C47.** A network administrator has modified all wireless access points to use WPA2 instead of WEP. Which of the following would be the main reason for this change?

- A.** Faster throughput
- B.** Better reception and range
- C.** Reduced power use
- D.** Better security

Quick  
Answer: **291**

The Details: **339**

**C48.** A help desk is receiving reports that a group of devices is not able to communicate outside of their local IP subnet. A technician can ping devices on the same network, but does not receive a response when pinging the IP address of external devices. Which of the following would be the MOST likely cause of this issue?

- A. Default gateway
- B. DNS server
- C. Proxy server
- D. QoS

Quick  
Answer: 291

The Details: 340

**C49.** A network technician has been tasked with preventing corporate laptops from connecting to a training room's wireless network. Which of the following would be the BEST way to accomplish this?

- A. Enable MAC filtering
- B. Use WPS
- C. Apply static IP addressing
- D. Create content filters

Quick  
Answer: 291

The Details: 341

**C50.** While working at a customer's desk, a technician's mobile phone begins to ring. Which of the following would be the MOST appropriate response?

- A. Take the call and address the caller's requests before continuing
- B. Take the call and ask the caller if you can return their call later
- C. Send the call to voicemail and apologize for the interruption
- D. Politely excuse yourself and step out to take the call

Quick  
Answer: 291

The Details: 342

**C51.** A user's workstation has been identified as participating in a DDoS to a large Internet service provider. The computer has been powered down and stored in a locked area until investigators arrive. Which of these procedures would be the MOST important to follow in the meantime?

- A.** Create documentation of the storage area
- B.** Retrieve logs from the workstation Event Viewer
- C.** Obtain the purchase records of the workstation
- D.** Maintain integrity of the workstation data

Quick  
Answer: 291

The Details: 343

**C52.** A system administrator has configured EFS on a user's workstation. Which of the following would describe this functionality?

- A.** Encryption of individual files and folders
- B.** Conservation of bandwidth to remote sites
- C.** Encrypted network tunnel
- D.** Full disk encryption

Quick  
Answer: 291

The Details: 344

**C53.** An application update has been installed to all computers in the accounting department. Sam, a user, starts the updated application for the first time but nothing appears on the screen. Which of the following would be the best NEXT troubleshooting step?

- A.** Reinstall the application
- B.** Add Sam to the Administrator's group
- C.** Install the latest Windows updates
- D.** Check the Event Viewer

Quick  
Answer: 291

The Details: 345

**C54.** A technician has been asked to work on an urgent computer repair while the user is at lunch. When the technician arrives, they notice paperwork on the desk that may contain private customer information. Which of the following would be the BEST next step?

- A.** Complete the repair as quickly as possible
- B.** Ask an associate in the department for assistance
- C.** Move the papers somewhere out of sight
- D.** Leave without repairing the computer

Quick  
Answer: 291

The Details: 346

**C55.** A company has recently been the victim of a storm with large-scale flooding, and all systems and backups at the corporate data center were completely destroyed. Which of the following would be the BEST way to avoid this loss of data in the future?

- A.** Uninterruptible power supplies
- B.** Cloud storage
- C.** RADIUS administration servers
- D.** Image-level backups

Quick  
Answer: **291**

The Details: **347**

**C56.** A user commonly stores large graphic image files in a shared folder on a network server. After logging in one morning, the user notices that the shared folders are no longer in the list of available storage drives. The user confirms that they are logged in properly to the Windows Domain. Which of the following would be the MOST likely reason for this issue?

- A.** User's permissions have been modified
- B.** User is running untrusted software
- C.** Network is using MAC filtering
- D.** Port security is enabled

Quick  
Answer: **291**

The Details: **348**

**C57.** A company deploys a suite of commercial software onto every workstation in the organization. Which of the following would BEST describe this licensing?

- A.** Personal licenses
- B.** Enterprise license
- C.** FOSS license
- D.** End user licensing agreement

Quick  
Answer: **291**

The Details: **349**

**C58.** A desktop administrator is troubleshooting an issue with a client's desktop computer that dual-boots between Windows and Linux. Due to a change in job requirements, the Linux operating system was removed from the desktop computer. Now when the computer is powered on, Windows does not start and the computer displays the message, "Missing operating system." The administrator has confirmed that the storage drive is operating properly, and when they boot with a Windows Preinstallation Environment they can see the user's data on the drive. Which of the following would be the BEST way to resolve this issue?

- A.** Modify the boot order in the BIOS
- B.** Reinstall the Windows operating system
- C.** Boot to Safe Mode and disable all startup applications
- D.** Reinstall the Windows boot manager

Quick  
Answer: **291**

The Details: **350**

**C59.** A user is working with a .dmg file on their macOS desktop. Which of the following would describe the contents of this file?

- A.** Debug information
- B.** Disk image
- C.** Application library
- D.** Disk maintenance utility

Quick  
Answer: **291**

The Details: **351**

**C60.** A member of the accounting department at headquarters is getting a new laptop and would like to reissue the older Windows 10 laptop to an accounting team member at a remote site. The headquarters user would like to remove all personal files, apps, and settings before sending the laptop to the remote site. Which of the following would be the BEST way to accomplish this?

- A.** Remove the Windows partition and reinstall
- B.** Perform a Windows 10 reset
- C.** Perform a secure wipe and reinstall from original Windows media
- D.** Uninstall all apps under Control Panel / Programs and Features

Quick  
Answer: **291**

The Details: **352**

**C61.** Walter, a user, has noticed that his computer begins to slow down during daily use and eventually locks up completely. During the lock up, the keyboard and mouse do not respond and the screen does not show any error messages. Which of the following tasks should a technician follow to BEST troubleshoot this issue? (Choose TWO)

- A. Start the computer in Safe Mode
- B. Perform a hardware diagnostic
- C. Connect the computer to a different VLAN
- D. Update the OS to the latest patches
- E. Roll back to a previous configuration
- F. Scan for viruses and malware

Quick  
Answer: 291

The Details: 353

**C62.** A user receives this message each time they visit a secure website: "The site's security certificate is not trusted." A technician investigates the issue and finds that the problem only occurs on this user's computer and not with other computers in the same office. Which of the following would be the best NEXT troubleshooting task?

- A. Disable Windows Firewall for all HTTPS traffic
- B. Create a new certificate for the user's computer
- C. Check the date and time on the user's computer
- D. Release and refresh the IP address configuration

Quick  
Answer: 291

The Details: 355

**C63.** A user's smartphone contains company confidential information that should not be shared outside of the organization. Which of the following would be the BEST way to limit access to this data if the smartphone was lost or stolen?

- A. PIN
- B. Remote wipe
- C. Swipe pattern
- D. Cloud backup

Quick  
Answer: 291

The Details: 356

**C64.** An IT organization has created a series of Windows 10 file share names that end with a dollar sign (\$). Which of the following would describe these shares?

- A. Optimized
- B. Hidden
- C. Remote
- D. Encrypted

Quick  
Answer: 291

The Details: 357

**C65.** A computer on a manufacturing floor has a virus, and the system administrator has removed the system from the company network. Which of the following virus removal tasks should occur NEXT?

- A. Discuss virus prevention with the end user
- B. Install the latest anti-virus signatures
- C. Schedule a virus scan to run each morning
- D. Disable System Restore

Quick  
Answer: 291

The Details: 358

**C66.** A user in the marketing department needs to move data between macOS and Windows computers using a USB flash drive. Which of the following file systems would be the BEST way to easily transfer files between these operating systems?

- A. exFAT
- B. HFS+
- C. NTFS
- D. NFS

Quick  
Answer: 291

The Details: 359

**C67.** When a user starts their desktop computer, the Windows splash screen is shown with a rotating circle, but the login screen is never displayed. A technician researches the issue and finds that the computer was just updated to the latest set of Windows patches. Which of the following would be the NEXT step the technician should follow to help solve this issue?

- A. Reconfigure the BCD settings
- B. Perform a Startup Repair
- C. Start in VGA mode
- D. Rebuild the user's profile

Quick  
Answer: 291

The Details: 360

**C68.** A desktop technician is moving hard drives from one set of training room computers to another. Which of the following would allow the drives to be used in the new computers but prevent any of the existing data from being recovered?

- A.** Shredder
- B.** Quick format
- C.** Drill
- D.** Standard format

Quick  
Answer: **291**

The Details: **361**

**C69.** A workstation technician manages a training center that contains thirty student computers in each room. All of the computers have the same hardware configurations. Which of these installation methods would be the BEST choice for quickly resetting the training rooms at the end of each week?

- A.** In-place upgrade
- B.** Image installation
- C.** Repair installation
- D.** Clean install

Quick  
Answer: **291**

The Details: **362**

**C70.** A user has asked a technician to repair the display on a smartphone that works normally every morning but is very dim in the afternoon. The technician has performed a soft reset but the display is still dim. Which of the following would be the MOST likely reason for this issue?

- A.** Power saving mode
- B.** Corrupted OS update
- C.** Non-working backlight
- D.** The battery is charging

Quick  
Answer: **291**

The Details: **363**

**C71.** A desktop technician is troubleshooting a user's laptop with very high utilization, even with no activity on the screen or user input to the operating system. Task Manager shows that the CPU is operating at 100% utilization, memory utilization is slightly elevated, and there is a large amount of outbound network communication. Which of the following would be the MOST likely reason for these issues?

- A.** System RAM is faulty
- B.** User has not properly authenticated
- C.** Laptop is part of a botnet
- D.** Network adapter is faulty

Quick  
Answer: **291**

The Details: **364**

**C72.** Daniel, a user in the marketing department, has been notified that other users have received email messages that show him as the sender, but he did not send the emails. There are no records of these emails in Daniel's sent messages folder. A technician researching the issue finds that Daniel's computer appears to be working properly and is not infected with any malicious software. Which of these should the technician check NEXT?

- A.** Email hijacking
- B.** Invalid email certificate
- C.** VLAN mismatch
- D.** Incorrect email server configuration

Quick  
Answer: **291**

The Details: **365**

**C73.** A company has created an internal process to ensure that all PII is encrypted. Which of the following would be the MOST likely reason for adding this additional security?

- A.** Helps prevent identity theft
- B.** Improves application performance
- C.** Allows customer data to be easily deleted
- D.** Uses less storage space

Quick  
Answer: **291**

The Details: **366**

**C74.** A system administrator is installing a file server into the corporate data center. Which of the following would be the BEST way to improve security of the file sharing service? (Select TWO)

- A. Enable a BIOS user password
- B. Connect the server to a wireless network
- C. Limit the number of concurrent connections
- D. Disable unused accounts
- E. Enable file storage quotas
- F. Enable password complexity

Quick  
Answer: **291**

The Details: **367**

**C75.** A user has purchased a computer that uses a 32-bit version of an operating system. Which of the following would be the maximum amount of RAM supported in this OS?

- A. 32 GB
- B. 2 TB
- C. 512 GB
- D. 128 GB
- E. 4 GB
- F. 16 GB

Quick  
Answer: **291**

The Details: **368**

**C76.** A financial services company is upgrading the storage drives on their SAN and need to dispose of one hundred older storage drives. The security administrator would like to guarantee all of the drives are destroyed and the data could not be recovered. Which of the following methods would be the BEST way to accomplish this goal?

- A. Standard format
- B. Full disk encryption
- C. Shredder
- D. Delete the master boot record

Quick  
Answer: **291**

The Details: **369**

**C77.** A company is updating all of their UPS systems with new batteries. Which of the following would be the best way to dispose of the old batteries?

- A.** Take to a local hazardous waste facility
- B.** Throw out with the paper trash
- C.** Ship them to a battery wholesaler
- D.** Bury them in a landfill

Quick  
Answer: **291**

The Details: **370**

**C78.** Which of the following should a company use to reduce their legal liability if an employee is dismissed?

- A.** End user licensing agreement
- B.** Acceptable use policy
- C.** Knowledge base articles
- D.** Operational procedures documentation

Quick  
Answer: **291**

The Details: **371**

**C79.** Jack, a healthcare administrator, commonly displays sensitive data on his screen as part of his normal work activities. His desk is in an open area near a busy hallway. Which of the following would add additional security to Jack's work area?

- A.** Biometric door lock
- B.** Privacy filter
- C.** Cable lock
- D.** Locking cabinet

Quick  
Answer: **291**

The Details: **372**

**C80.** Walter, a user, is trying to use a new stylus with his tablet. The screen on the tablet responds to a finger press or a swipe, but the stylus does not interact with the tablet screen. Which of the following would be the MOST likely fix for this issue?

- A.** Connect to a power source
- B.** Enable Bluetooth
- C.** Upgrade to the latest OS version
- D.** Disable the Wi-Fi network

Quick  
Answer: **291**

The Details: **373**

- C81.** A network administrator has been asked to manage the router configurations at all company remote locations. Which of the following would be the BEST choice for this task?
- A. SSH
  - B. VNC
  - C. Telnet
  - D. RDP
- C82.** A user is browsing to their corporate home page, but a different website appears instead. The user tries to connect with other browsers on the same computer, but the result is identical. Which of the following would be the best NEXT troubleshooting step?
- A. Try connecting to the site in Safe Mode
  - B. Perform an anti-malware scan
  - C. View all browsing results in the Event Viewer
  - D. Roll back to a previous configuration
- C83.** A technician has just received fifty boxes of used laser printer toner cartridges that were removed during an annual preventive maintenance project. Which of the following would be the best NEXT step for managing these used cartridges?
- A. Refer to the MSDS
  - B. Ship the cartridges to the original manufacturer
  - C. Dispose of the cartridges with the rest of the trash
  - D. Drill a hole in each cartridge

Quick  
Answer: 291

The Details: 374

Quick  
Answer: 291

The Details: 375

Quick  
Answer: 291

The Details: 376

**C84.** A system administrator has been notified that a serious security vulnerability has been identified in software used by the company. In order to quickly patch this vulnerability, the administrator has created change management documentation that will be presented to the change board. Which part of the documentation would explain the disadvantages of not quickly patching this software?

- A.** Backout plan
- B.** End-user acceptance
- C.** Detailed change plan
- D.** Risk analysis

Quick  
Answer: **291**

The Details: **377**

**C85.** A company is donating ten laptop computers to a local community center. Which of the following processes should be followed before making this donation?

- A.** Inventory management
- B.** Acceptable use policy
- C.** Password policy
- D.** Knowledge base article

Quick  
Answer: **291**

The Details: **378**

**C86.** A desktop technician would like to reinstall the Windows 10 operating system without removing any of the personal files and settings on the computer. Which of the following would be the BEST way to complete this process?

- A.** Clean installation
- B.** Unattended installation
- C.** Multiboot
- D.** Refresh

Quick  
Answer: **291**

The Details: **379**

**C87.** A security administrator is configuring VPN connectivity on the company smartphones and tablets. The administrator would like to ensure that the login requests are from corporate users and not unauthorized third-parties. Which of the following would provide this security feature?

- A.** Biometrics
- B.** PIN
- C.** Unique usernames
- D.** Passcode

Quick  
Answer: **291**

The Details: **380**

**C88.** A company is moving three computer racks of equipment from an old data center to a new facility. Which of these safety features should be the MOST important requirement at the new location?

- A.** Air filter masks
- B.** Anti-static mat
- C.** Equipment grounding
- D.** Surge protectors

Quick  
Answer: **291**

The Details: **381**

**C89.** A system administrator needs to upgrade five computers at a remote site to Windows 10. Which of the following methods would perform these upgrades without requiring any input from the users?

- A.** Clean install
- B.** Multiboot
- C.** Unattended installation
- D.** Repair installation

Quick  
Answer: **291**

The Details: **382**

**C90.** Which of the following would allow someone else in the room to maliciously obtain a username and password?

- A.** Spoofing
- B.** Tailgating
- C.** DoS
- D.** Shoulder surfing

Quick  
Answer: **291**

The Details: **383**





# Practice Exam C

## Multiple Choice Quick Answers

- |        |              |              |
|--------|--------------|--------------|
| C6. C  | C36. B       | C66. A       |
| C7. A  | C37. D       | C67. B       |
| C8. D  | C38. A       | C68. D       |
| C9. C  | C39. D       | C69. B       |
| C10. C | C40. B       | C70. A       |
| C11. C | C41. C       | C71. C       |
| C12. A | C42. C       | C72. A       |
| C13. C | C43. B       | C73. A       |
| C14. A | C44. C       | C74. D and F |
| C15. D | C45. D       | C75. E       |
| C16. C | C46. D       | C76. C       |
| C17. D | C47. D       | C77. A       |
| C18. B | C48. A       | C78. B       |
| C19. C | C49. A       | C79. B       |
| C20. A | C50. C       | C80. B       |
| C21. A | C51. D       | C81. A       |
| C22. A | C52. A       | C82. B       |
| C23. D | C53. D       | C83. A       |
| C24. B | C54. B       | C84. D       |
| C25. B | C55. B       | C85. A       |
| C26. B | C56. A       | C86. D       |
| C27. D | C57. B       | C87. A       |
| C28. D | C58. D       | C88. C       |
| C29. B | C59. B       | C89. C       |
| C30. D | C60. B       | C90. D       |
| C31. A | C61. B and F |              |
| C32. D | C62. C       |              |
| C33. D | C63. B       |              |
| C34. C | C64. B       |              |
| C35. C | C65. D       |              |



# Practice Exam C

## Detailed Answers

- C1. A Windows desktop administrator would like to query the local DNS server to view the IP address and for www.professormesser.com. Use a command line utility to view this information.



```
Command Prompt

C:\>nslookup www.professormesser.com
Server: dns9.quad9.net
Address: 9.9.9.9

Non-authoritative answer:
Name: www.professormesser.com
Addresses: 104.22.73.108
          172.67.41.114
          104.22.72.108

C:\>
```

The nslookup (name server lookup) command can be used to query a DNS server for information about IP addresses, fully qualified domain names, email server addresses, and other important name services.



### More information:

220-1002, Section 1.4 - Network Command Line Tools  
<https://professormesser.link/1002010402>

**C2.** Match the Linux command to the description.

Some descriptions will not have a match.

**Commands:**

mv

**Descriptions:**

Rename a directory

The mv (move) command is used to "move" a file from one location to another, or from one name to another.

pwd

Display the current working directory path

The pwd (Print Working Directory) command will display the current working directory path.

chmod

Make a file read-only

Chmod (Change Mode) allows the user to change the access (mode) of a file to read, write, execute, or a combination of those permissions.

grep

Search through files for the word "transaction"

The grep command can search through many files and directories to locate a pattern. This is commonly used to locate specific text strings.

passwd

Change a user's password

The passwd (password) command is used to change a Linux user's password.

chown

Modify the owner of a file

The chown (Change Owner) command is used to modify the file owner or group owner assignment.

sudo

Run a program with elevated permissions

The sudo command will allow the user to execute a command as the superuser or as another account on the system.



**More information:**

220-1002, Section 1.9 - Basic Linux Commands

<https://professormesser.link/1002010906>

- C3.** A user has contacted the help desk because they are not able to browse any websites. What command line utility would be able to confirm the connectivity to a server that could convert fully qualified domain names to IP addresses?

```
Command Prompt
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 10.1.10.45(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, July 28, 2020 10:52:39 AM
Lease Expires . . . . . : Tuesday, August 4, 2020 10:55:08 AM
Default Gateway . . . . . : 10.1.10.1
DHCP Server . . . . . : 10.1.10.1
DNS Servers . . . . . : 9.9.9.9
NetBIOS over Tcpip. . . . . : Enabled

C:\>ping 9.9.9.9

Pinging 9.9.9.9 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 9.9.9.9:
  Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

The device that converts between fully qualified domain names and IP addresses is the DNS (Domain Name System) server. The nslookup results show the configured DNS server is located at 9.9.9.9, and the ping command is the easiest way to confirm the connectivity of the device.



#### More information:

220-1002, Objective 1.4 - Network Command Line Tools  
<https://professormesser.link/1002010402>

---

- C4.** An application, foothold.exe, has become unresponsive and the user is not able to close the application normally from the Windows desktop. Use the Windows command line to terminate this application.



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command "C:\>taskkill /im foothold.exe" is entered, followed by the output "SUCCESS: Sent termination signal to the process \"foothold.exe\" with PID 8156.". The prompt "C:\>" is visible at the bottom.

The "taskkill" command is used to terminate tasks at the command line. The /IM option specifies an "image name" or application name. If the process ID is known, the taskkill command can be used with the /PID option and /T (terminate) option.



**More information:**

220-1002, Section 1.4 - Microsoft Command Line Tools

<https://professormesser.link/1002010401>

---

**C5.** Match the Control Panel applet to the description.

Some descriptions will not have a match.

**Applets:**

**Descriptions:**

User Accounts	Change an account to an Administrator
---------------	---------------------------------------

The User Accounts applet is used to modify user rights, passwords, certificate information, and more.

File Explorer Options	Disable indexing of system directories
-----------------------	--

The Windows 10 File Explorer Options control the general operation of File Explorer, the file viewing options, and search engine configurations.

Credential Manager	Save a website username and password
--------------------	--------------------------------------

Credential Manager is used to store, view, and delete authentication details for local devices, applications, and websites.

Device Manager	Disable a USB audio controller
----------------	--------------------------------

Device Manager is the central management view of all hardware and devices connected to the system. All device drivers can be enabled and disabled from the Device Manager applet.

BitLocker	Protect all data saved on a volume
-----------	------------------------------------

BitLocker provides full disk encryption for Windows volumes.

Internet Options	View website certificates
------------------	---------------------------

The Content tab of the Internet Options applet can be used to manage browser certificates.

Sync Center	Update a spreadsheet when away from the office
-------------	--

Sync Center makes files available when working offline, and synchronizes the changes when back online.



**More information:**

220-1002, Section 1.6 - The Windows Control Panel

<https://professormesser.link/1002010601>

**C6.** A technician has been called to resolve an issue with a desktop computer in a training facility. The computer appears to boot properly to the desktop, but applications take five minutes to load. While using the application, pop-up messages and other windows appear on the desktop. Which of the following should be the best NEXT troubleshooting step?

- A.** View running processes in Task Manager
  - B.** Disable System Restore
  - C.** Remove the computer from the network
  - D.** Educate the end user
- 

**The Answer:** **C.** Remove the computer from the network

The first step after identifying a potential malware infection is to quarantine the system to prevent the unintended spread of the malware.

**The incorrect answers:**

**A.** View running processes in Task Manager

The analysis and removal of the malware can begin once the system has been removed from the network and completely quarantined.

**B.** Disable System Restore

Before attempting to remove the malware, it's important to disable the System Protection feature to remove any infected restore points. This step should be completed after the system has been quarantined.

**D.** Educate the end user

Once the malware removal process is complete, the last step is to educate the end user to help prevent this type of infection in the future.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**C7.** A system administrator would like to disable the TFTP Client in Windows 10. Which of the following Control Panel applets would be the BEST choice for this task?

- A.** Programs and Features
  - B.** Services
  - C.** Credential Manager
  - D.** File Explorer options
- 

**The Answer:** **A.** Programs and Features

The Programs and Features applet of the Control Panel is used to view and manage installed applications, or to enable or disable individual Windows features.

**The incorrect answers:**

**B.** Services

The Services utility would allow the administrator to disable a TFTP service, or any other Windows service. To remove a client or Windows feature, the administrator would need to use Programs and Features.

**C.** Credential Manager

The Credential Manager stores the usernames and passwords used on Windows resources and websites. The Credential Manager does not manage the use of different Windows utilities and programs.

**D.** File Explorer options

The File Explorer options are used to customize the options available in the File Explorer, change the view in the window, and modify the Windows search options. File Explorer does not control the use of individual applications.



**More information:**

220-1002, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1002010601>

**C8.** A user has noticed that a Bluetooth device is currently connected to their tablet, but they don't recognize the make or model of the connected device. Which of the following would be the FIRST step for troubleshooting this issue?

- A.** Perform an anti-malware scan
  - B.** Research installed apps with an app scanner
  - C.** Disable the Wi-Fi network
  - D.** Remove the Bluetooth device
- 

**The Answer:** **D.** Remove the Bluetooth device

Before continuing, the most important step is to ensure that the connected device no longer has access to the system. Removing the Bluetooth device from the list of paired devices would be the safest first option.

**The incorrect answers:**

**A.** Perform an anti-malware scan

An anti-malware scan might be needed, but it would not be the best first step for troubleshooting this issue. Before doing anything else, the device should be removed.

**B.** Research installed apps with an app scanner

There's no evidence that an installed app is associated with this paired Bluetooth device, so researching apps would not be the best first step.

**C.** Disable the Wi-Fi network

This issue is related to the Bluetooth network, so disabling the Wi-Fi network configuration would have no effect.



**More information:**

220-1002, Objective 3.5

Troubleshooting Mobile Device Security

<https://professormesser.link/1002030501>

**C9.** A user has recently been assigned a new tablet, but each time she tries to read email messages she receives the message, “The email could not be decrypted.” The user has reinstalled the email client, but the problem still occurs over both Internet and VPN connections. Which of the following would be the best way for a technician to resolve this issue?

- A.** Ask the user to reset their password
  - B.** Change the user's email alias
  - C.** Send the user a certificate with a private key
  - D.** Confirm the wireless network encryption settings
- 

**The Answer:** **C.** Send the user a certificate with a private key

A problem with email decryption is most likely associated with the decryption keys. If the keys are missing or are incorrect, then the local device will not be able to view the email messages.

**The incorrect answers:**

**A.** Ask the user to reset their password

If the user is properly authenticated, then the issue is not related to the password. Resetting the password would not provide any additional access to the email messages.

**B.** Change the user's email alias

The user's email alias provides other options for sending messages, but it would not provide any additional method of decrypting email messages.

**D.** Confirm the wireless network encryption settings

The wireless network is not part of the email client's encryption process. Confirming or modifying wireless network configurations will not resolve this issue.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**C10.** A computer technician has been asked to verify a set of new Group Policy settings on computers at a remote site. Which of the following commands should be used to validate the last policy update on the systems?

- A. net view
  - B. sfc
  - C. gpresult
  - D. netstat
  - E. dism
- 

**The Answer:** C. gpresult

The gpresult (Group Policy Results) utility will display the policy settings associated with a computer or user.

**The incorrect answers:**

**A. net view**

The net view command displays a list of network resources and shares available on a Workgroup or Windows Domain.

**B. sfc**

The sfc (System File Checker) command will scan the integrity of all protected system files and repair any that may be damaged.

**D. netstat**

The netstat (Network Statistics) command can display active connections, routing tables, and other network traffic metrics. The netstat command is not associated with Group Policy settings.

**E. dism**

The dism (Deployment Image Servicing and Management) utility is used for managing and configuring Windows Imaging Format (WIM) files.



**More information:**

220-1002, Objective 1.4 - Microsoft Command Line Tools  
<https://professormesser.link/1002010401>

**C11.** A system administrator needs to modify the Linux group associated with a file. Which of the following would provide this functionality?

- A.** ps
  - B.** ifconfig
  - C.** chown
  - D.** grep
- 

**The Answer:** **C.** chown

The chown (Change Owner) command will modify the owner or group associated with a file system object.

**The incorrect answers:**

**A. ps**

The ps (List Processes) command will display a list of the running processes on a Linux computer. The ps command does not display group information relating to a file.

**B. ifconfig**

The ifconfig (Interface Configuration) command can view or configure a network interface and IP configuration in Linux.

**D. grep**

The grep command is used to find text in a file. Many files can be searched simultaneously, and the resulting matches are displayed to the Linux console.



**More information:**

220-1002, Objective 1.9 - Basic Linux Commands

<https://professormesser.link/1002010906>

**C12.** A user has brought their laptop to the help desk because of an issue during startup. The laptop screen remains black when powering on, and no status lights appear on the system. The user is traveling tomorrow to a remote site in another country and needs the laptop while they are on the road. Which of the following would be the best NEXT choice?

- A.** Provide the user with the option to repair, replace, or rent a new system
  - B.** Assign the user to the standard seven-day repair agreement
  - C.** Replace the external power cable and close the repair ticket
  - D.** Recommend the user cancel their travel plans
- 

**The Answer:** **A.** Provide the user with the option to repair, replace, or rent a new system

Given the short timeframe available for repair, it would be useful to provide the customer with some options that would allow them to travel internationally with a working laptop. The user can then decide the best way to proceed.

**The incorrect answers:**

**B.** Assign the user to the standard seven-day repair agreement

The user is traveling the following day, so assigning a seven-day repair priority would not provide them with a laptop during their trip.

**C.** Replace the external power cable and close the repair ticket

There's no evidence that the power cable is the issue, so replacing the cable and closing the ticket would not provide the user with the best possible outcome.

**D.** Recommend the user cancel their travel plans

Asking the user to cancel an international trip without any knowledge of the trip would be an uninformed decision and an unprofessional suggestion. The primary goal should be to find a way to provide the user with a laptop given the travel requirement.



#### More information:

220-1002, Objective 4.7 - Communication

<https://professormesser.link/1002040701>

**C13.** A home user provides numerous online presentations during the day, but the power in their area is not stable and there will often be short power outages. Which of the following would help with this issue?

- A.** Cloud backups
  - B.** External storage device
  - C.** UPS
  - D.** Surge suppressor
- 

**The Answer: C. UPS**

A UPS (Uninterruptible Power Supply) can provide ongoing backup power with the main power source is unavailable. This is especially useful for areas where power outages may be numerous and ongoing.

**The incorrect answers:**

**A.** Cloud backups

Copying files to the cloud is a useful backup strategy, but it doesn't provide any protection or recovery if the main power is not available.

**B.** External storage device

An external storage device can be used to store files separately from the main computer, but it doesn't prevent downtime or data loss if the primary power source fails.

**D.** Surge suppressor

A surge suppressor will remove any voltage spikes or noise from the electrical line, but it won't be useful if the primary power source is not available.



**More information:**

220-1002, Objective 4.3 - Disaster Recovery

<https://professormesser.link/1002040301>

**C14.** A system administrator is planning to upgrade two physical servers in the corporate data center to external cloud-based platforms. Which of the following would provide information on connectivity and the plans for remote site access?

- A.** Change scope
  - B.** End-user acceptance
  - C.** Backout plan
  - D.** Risk analysis
- 

**The Answer:** **A.** Change scope

When making a change, the details of the modifications must be well documented as part of the change scope. The change scope would include all of the systems affected by the change, the timeframe for completing the change, and any other important details about the modification.

**The incorrect answers:**

**B.** End-user acceptance

Prior to making any changes, the end-users must provide approvals for the update. This ensures that the users are involved in the change control process and they understand the scope of the change.

**C.** Backout plan

Every proposed change needs a documented method of reverting back to the original state. Unexpected problems often occur, so it's important to have a way to return everything back to their original forms.

**D.** Risk analysis

Every change (or lack of change) involves some level of risk. The change control process should also include an analysis of this risk.



**More information:**

220-1002, Objective 4.2 - Change Management

<https://professormesser.link/1002040201>

**C15.** A system administrator would like to conserve bandwidth to remote sites connected over slower network links. Which of these Windows features would provide this functionality?

- A.** EFS
  - B.** Domain Services
  - C.** BitLocker
  - D.** BranchCache
- 

**The Answer:** **D.** BranchCache

BranchCache is a Windows feature that caches information at remote offices without additional hardware or external services. The process is seamless to the end user and integrates into the existing Windows infrastructure.

**The incorrect answers:**

**A.** EFS

EFS (Encrypting File System) is a feature that encrypts file system objects on a Windows computer. EFS does not provide any features to save bandwidth.

**B.** Domain Services

Domain Services describes a centralized management function of the Windows operating system. Larger networks use Domain Services to easily manage all of the Windows systems on the network.

**C.** BitLocker

BitLocker is a Windows feature providing full disk encryption of entire volumes. BitLocker does not conserve bandwidth over slower links.



**More information:**

220-1002, Objective 1.2 - Windows in the Enterprise

<https://professormesser.link/1002010204>

**C16.** A user has just installed a driver update from a laptop manufacturer. After restarting, their system shows a Windows Stop Error before the login prompt is displayed. Each subsequent reboot causes the same error to be displayed. Which of the following should the system administrator follow to BEST resolve this issue?

- A. Modify the BIOS boot order
  - B. Boot to Safe Mode and perform a Windows Reset
  - C. Perform a System Restore
  - D. Reinstall the patch files
- 

**The Answer:** C. Perform a System Restore

A System Restore can be launched from the Advanced Boot Options under Repair Your Computer. From there, you can select an existing restore point that will restore the computer to a previous configuration.

**The incorrect answers:**

**A. Modify the BIOS boot order**

The BIOS boot order will change the priority for storage drives during the startup process. This issue appears to be related to a device driver and not to a specific startup drive.

**B. Boot to Safe Mode and perform a Windows Reset**

Although Safe Mode may allow a user to login and avoid the reboot problem, performing a Windows Reset would be a significant change to the operating system. A Reset will reinstall Windows and can delete files, settings, and apps that were not included with the computer.

**D. Reinstall the patch files**

Since the problem occurred when the patch files were installed, installing them again wouldn't be advisable. It's also difficult to reinstall the patch files if the user can't login to the computer.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Solutions  
<https://professormesser.link/1002030102>

**C17.** The available storage space on a user's workstation is running low, and some updates are failing due to insufficient drive space. Which of the following would be the BEST way to increase drive space until a larger storage drive can be installed?

- A.** Use a Guest login
  - B.** Enable System Protection
  - C.** Disable Remote Assistance
  - D.** Set the paging file size to zero
- 

**The Answer:** **D.** Set the paging file size to zero

The paging file is used with your system RAM to keep the applications performing at peak efficiency. Although disabling the paging file may affect the performance of a computer, it will free up all of the storage space that's normally reserved for the swap file.

**The incorrect answers:**

**A.** Use a Guest login

The type of login used on a computer does not generally affect the amount of free storage space on the computer.

**B.** Enable System Protection

The Windows System Protection feature will set restore points and save files and configurations to the storage drive. Enabling this feature will use more storage space, not less.

**C.** Disable Remote Assistance

The Remote Assistance feature is used to provide third-party remote control to the Windows desktop. Disabling this feature does not provide any significant change to the amount of free storage space on the drive.



**More information:**

220-1002, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1002010601>

**C18.** A technician is troubleshooting a Windows 10 computer that is performing very slowly when moving from one application to another. Which of the following utilities would allow the technician to view real-time resource activity?

- A.** Services
  - B.** Task Manager
  - C.** System Information
  - D.** Device Manager
- 

**The Answer:** **B.** Task Manager

The Windows Task Manager provides a real-time view of CPU utilization, memory usage, network throughput, and more.

**The incorrect answers:**

**A.** Services

The Services utility allows the administrator to enable, disable, and configure non-interactive Windows Services.

**C.** System Information

The System Information utility displays hardware resource configurations, component details, and software information. The System Information utility does not provide a real-time view of performance metrics.

**D.** Device Manager

The Device Manager is the central console for managing all hardware device drivers. The Device Manager does not provide any information on real-time system performance.



**More information:**

220-1002, Objective 1.5 - Windows Administrative Tools  
<https://professormesser.link/1002010501>

**C19.** An attacker has gained access to a password hash file. Which of the following will the attacker use to obtain the passwords?

- A. DoS
  - B. Decryption
  - C. Brute force
  - D. Phishing
- 

**The Answer:** C. Brute force

Since a hash is a one-way cryptographic method, the only way to determine the original plaintext is to try every possible combination until the hash is matched. This brute force method is the only way to determine the original source of the hash.

**The incorrect answers:**

**A. DoS**

A DoS (Denial of Service) would cause a service to be unavailable to others. A DoS attack would not determine the original passwords based on a hash.

**B. Decryption**

A hash is a one-way function and it's not encrypted data, so there's no option available for decrypting the passwords.

**D. Phishing**

Phishing is a social engineering method that convinces someone to willingly provide secret or private information. Performing a brute force attack on a hash file is not a method of phishing.



**More information:**

220-1002, Objective 2.5 - Brute Force Attacks

<https://professormesser.link/1002020505>

**C20.** A server administrator needs to create a folder on a Windows server to store weekly status report documents. Which of the following command-line tools would provide this functionality?

- A.** mkdir
  - B.** net use
  - C.** cd
  - D.** dir
  - E.** ls
- 

**The Answer:** **A.** mkdir

The mkdir (Make Directory) command is used to create a subdirectory or folder on the file system. The mkdir command is used in both Windows and Linux.

**The incorrect answers:**

**B.** net use

The net command is used for many different Windows-related functions, and the net use option will associate a drive letter with a Windows share.

**C.** cd

The cd (Change Directory) command is used to change the current command line context to a different working directory. The cd command is used in both Windows and Linux.

**D.** dir

The Windows dir (Directory) command is used to provide a list of the files and objects in the file system.

**E.** ls

The ls (list directory) command is used to view the files and objects in the Linux file system. This is the Linux equivalent of the Windows dir command.



**More information:**

220-1002, Objective 1.4 - Microsoft Command Line Tools

<https://professormesser.link/1002010401>

**C21.** A desktop administrator is troubleshooting a laptop computer experiencing slowdowns and delays during normal operation. There are many icons displayed at the bottom of the Windows desktop, and an error message on the screen shows “Out of memory or system resources.” Which of the following troubleshooting steps would be the BEST way to address this issue?

- A.** Use Task Manager to close applications
  - B.** Reboot the computer
  - C.** Release and renew the network connection
  - D.** Roll back to a previous restore point
- 

**The Answer:** **A.** Use Task Manager to close applications

A large number of icons at the bottom of the screen indicates that many applications are running, and the message complaining of available resources is most likely a result of this increased system load. Closing some of the applications should provide additional resources and help regain control of the operating system.

**The incorrect answers:**

**B.** Reboot the computer

Rebooting the computer would be an extreme solution that has the potential for losing data in the current system state. Regaining control of the system prior to rebooting would be ideal.

**C.** Release and renew the network connection

This issue doesn't appear to be related to the network, so resetting the network address assignments would not provide a resolution.

**D.** Roll back to a previous restore point

This issue appears to be related to the number of applications in use and not to a configuration or device driver error. Restoring an older configuration would most likely not be a long-term solution for this problem.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Solutions

<https://professormesser.link/1002030102>

**C22.** A desktop administrator is removing a virus from a laptop computer in a shared lab. The computer has been removed from the network and the System Restore feature has been disabled. When the administrator attempts to update to the latest anti-virus signatures, the anti-virus utility disables itself. Which of the following would be the best NEXT step?

- A.** Boot to Safe Mode and use signatures downloaded from a separate computer
  - B.** Roll back to a previous configuration
  - C.** Schedule periodic updates and reconnect to the network
  - D.** Discuss anti-virus strategies with the end user
- 

**The Answer:** **A.** Boot to Safe Mode and use signatures downloaded from a separate computer

It's not uncommon for viruses to disable access to recovery software. To work around this issue, a technician may often need to restart in Safe Mode and copy utilities and recovery files from a different computer.

**The incorrect answers:**

**B.** Roll back to a previous configuration

Viruses often infect both the current configuration and those contained in restore points. In this case, the System Restore feature has already been disabled, so no restore points would be available on this system.

**C.** Schedule periodic updates and reconnect to the network

Since the manual update process is failing, it's most likely an automated update would also fail.

**D.** Discuss anti-virus strategies with the end user

Once the virus has been removed and the system is set to automatically update and scan for viruses, the technician can educate the end user about ways to avoid this problem in the future.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**C23.** A Windows 10 computer is displaying a series of error messages during the startup process. A technician has been dispatched and would like to view more information about the errors without restarting the computer. Which of the following utilities would provide the technician with more details about these messages?

- A.** taskschd
  - B.** devmgmt
  - C.** perfmon
  - D.** eventvwr
  - E.** sfc
- 

**The Answer:** **D.** eventvwr

The Windows eventvwr (Event Viewer) provides a historical log of all system and application events. The error messages seen previously on the system can be found in the Event viewer.

**The incorrect answers:**

**A. taskschd**

The taskschd (Task Scheduler) is used to automate a task at a specific date and time. This allows the user to update the system, download files, or perform any other function without any user intervention.

**B. devmgmt**

The Windows devmgmt (Device Manager) provides access to the hardware device drivers.

**C. perfmon**

The perfmon (Performance Monitor) gathers performance metrics over time to provide a graphical view of trends.

**E. sfc**

The sfc (System File Checker) utility will scan the integrity of protected system files and repair files that may be corrupted.



**More information:**

220-1002, Objective 1.5 - Windows Administrative Tools

<https://professormesser.link/1002010501>

**C24.** A user's corporate smartphone has stopped responding to screen touches or button presses. Which of the following would be the BEST way to resolve this issue?

- A.** Connect the smartphone to a power source
  - B.** Perform a hard reset
  - C.** Reset the Internet router
  - D.** Power off all Bluetooth devices
- 

**The Answer:** **B.** Perform a hard reset

There aren't a lot of options for a device that won't respond to any input. The best way to regain control would be to perform a reset and continue the troubleshooting once the device restarts.

**The incorrect answers:**

**A.** Connect the smartphone to a power source

Providing a power source would not commonly restore access to the touch screen.

**C.** Reset the Internet router

It's unlikely that the touch screen issue is related to a problem on a different device. Restarting the Internet router would not commonly correct any input issues on the smartphone.

**D.** Power off all Bluetooth devices

It would be unusual for Bluetooth devices to cause these input problems. Powering off those Bluetooth devices would not provide any additional access to the smartphone.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**C25.** Jack, a technician, has been asked to replace a faulty adapter card in a server. Jack does not have an anti-static strap to use for this repair, but he has removed the server from a power source. Which of the following would be the BEST way to safely complete this repair?

- A. Store the faulty card in an anti-static bag
  - B. Periodically touch the server's metal chassis
  - C. Wear safety goggles
  - D. Have a carbon dioxide extinguisher nearby
- 

**The Answer:** B. Periodically touch the server's metal chassis

If an anti-static strap isn't available to maintain a constant connection between a person and the equipment they're working on, the next-best option would be to occasionally touch some metal on the device to equalize the electrical potential and prevent ESD (electrostatic discharge).

**The incorrect answers:**

A. Store the faulty card in an anti-static bag

It's important to protect all components, but a known-bad component doesn't have the same priority as the new, working component.

C. Wear safety goggles

There isn't a danger from debris or eye damage when replacing an adapter card, so wearing safety goggles would not be necessary.

D. Have a carbon dioxide extinguisher nearby

The server has been disconnected from power, so there would not be a fire concern when replacing the adapter card. Of course, it's a good idea to always know where the nearest extinguisher might be.



**More information:**

220-1002, Objective 4.4 - Managing Electrostatic Discharge

<https://professormesser.link/1002040402>

**C26.** Which of the following would be the BEST choice for a system administrator to manage an Active Directory database?

- A. Batch file
  - B. PowerShell
  - C. JavaScript
  - D. Visual Basic Scripting
- 

**The Answer:** B. PowerShell

PowerShell is Microsoft's command line scripting environment that provides integration into the Windows operating system and the control to automate almost every aspect of Windows.

**The incorrect answers:**

**A. Batch file**

A batch file provides access to the Windows file system, but it does not directly integrate with a Microsoft Active Directory database.

**C. JavaScript**

JavaScript is commonly used in a browser to customize aspects of the user interface or a website. JavaScript would not be the first choice to manage an Active Directory database.

**D. Visual Basic Scripting**

Visual Basic Scripting provides general purpose scripting in Windows, and very commonly in Microsoft Office applications. Visual Basic Scripting would not be the best choice for Active Directory automation.



**More information:**

220-1002, Objective 4.8 - Scripting

<https://professormesser.link/1002040801>

**C27.** Jack, a user, has started his computer and received this message on the screen:

“Your important files are encrypted. If you want to decrypt all of your files, you need to pay.”

Sam, a desktop administrator, has confirmed that Jack can no longer access his desktop, and none of his installed applications are available in the system menus. Sam notices that a payment link is posted at the bottom of the screen. Which of the following would BEST describe this scenario?

- A. Spyware
  - B. Boot sector virus
  - C. Rootkit
  - D. Crypto-malware
- 

**The Answer: D. Crypto-malware**

Crypto-malware is ransomware that encrypts data files and requires payment before the files can be decrypted.

**The incorrect answers:**

**A. Spyware**

Spyware is malware that monitors your activity and shares the information with a third-party. This can often include browser sites, keylogging, and video monitoring.

**B. Boot sector virus**

A boot sector virus is malware that infects the boot sector or partition table of a drive. Once the system is started, the boot sector virus can infect the operating systems and storage devices on the computer.

**C. Rootkit**

A rootkit often resides in the kernel of an operating system and is effectively invisible to the operating system.



**More information:**

220-1002, Objective 2.4 - Types of Malware

<https://professormesser.link/1002020401>

**C28.** A desktop technician has received a complaint that a remotely-hosted application has stopped working. The technician believes that a network outage at the application provider is the root cause of the issue. Which of the following tools would be the BEST choice to confirm the location of the outage?

- A. ping
  - B. nslookup
  - C. netstat
  - D. traceroute
- 

**The Answer:** D. traceroute

The traceroute utility will show the network routes between two devices. If the route is disrupted between those two devices, the last available router will be identified.

**The incorrect answers:**

**A. ping**

The ping command will report if a device on the network can respond to the ping request, but it does not provide any location details if the device does not respond.

**B. nslookup**

The nslookup (Name Server Lookup) command will query a DNS (Domain Name System) server to identify IP addresses and fully qualified domain names. The nslookup command does not provide any information about network traffic or outages.

**C. netstat**

The netstat command will display connections, routes, and other network statistics associated with a single device. The netstat command does not provide any information about the uptime and availability of a remote network connection.



**More information:**

220-1002, Objective 1.4 - Network Command Line Tools  
<https://professormesser.link/1002010402>

**C29.** Users on the corporate network authenticate once at the beginning of the day, and are not prompted again for authentication until the following day. Which of the following would BEST describe this functionality?

- A. NTFS
  - B. SSO
  - C. Inherited permissions
  - D. EFS
- 

**The Answer: B. SSO**

SSO (Single Sign-On) requires the user to authenticate one time and have continued access to resources without requiring subsequent authentication requests. Windows Active Domain manages this SSO process through the use of the Kerberos network authentication protocol.

**The incorrect answers:**

**A. NTFS**

NTFS (NT File System) is a file system commonly used by Windows devices. NTFS does not provide any single sign-on capabilities or enhanced authentication features.

**C. Inherited permissions**

File permissions propagated from the parent object are called inherited permissions. The permissions assigned by the file system do not provide any enhanced single sign-on features.

**D. EFS**

EFS (Encrypting File System) is an NTFS feature that provides the ability to encrypt a group of files or folders without requiring the encryption of the entire volume. EFS does not provide any ongoing single sign-on functionality.



**More information:**

220-1002, Objective 2.6 - Windows Security Settings

<https://professormesser.link/1002020601>

**C30.** A server technician is removing the memory from a web server and adding new memory modules to the motherboard. The old memory modules will be used to upgrade a server in a different data center. Which of the following would be the BEST way to protect the old memory modules?

- A. Padded envelope
  - B. Cotton fabric
  - C. Molded foam packing material
  - D. Anti-static bag
- 

**The Answer:** D. Anti-static bag

An anti-static bag will protect sensitive electronic components from ESD (Electrostatic Discharge). This is important when moving components from one location to another, especially when an anti-static strap or anti-static pad cannot be used.

**The incorrect answers:**

**A.** Padded envelope

A padded envelope would provide some physical protection for the memory modules, but it would not protect the modules from the damaging results of an electrostatic discharge.

**B.** Cotton fabric

Cotton is a good way to provide physical protection, but it does not minimize the damage from a potential electrostatic discharge.

**C.** Molded foam packing material

Molded foam would provide physical protection for the components, but it would not protect against electrostatic discharge. The best of the available options would include an anti-static bag.



**More information:**

220-1002, Objective 4.4 - Managing Electrostatic Discharge  
<https://professormesser.link/1002040402>

**C31.** A Linux administrator is using the grep command while monitoring a database application. Which of the following would BEST describe this activity?

- A.** Search through a file for specific text
  - B.** View a list of running processes
  - C.** Change the permissions of a file
  - D.** View the name of the working directory
- 

**The Answer:** **A.** Search through a file for specific text

The grep command is used to search through a file or set of files for specific text.

**The incorrect answers:**

**B.** View of list of running processes

The ps (Process List) command is commonly used to view all of the running processes on a Linux computer. This is similar in functionality to the Windows Task Manager.

**C.** Change the permissions of a file

The Linux chmod (Change Mode) command is used to change the permissions of a file for the file owner, the file group, and everyone else.

**D.** View the name of the working directory

The pwd (Print Working Directory) command is used to display the current working directory path. This command is the same in both Windows and Linux.



#### More information:

220-1002, Objective 1.9 - Basic Linux Commands

<https://professormesser.link/1002010906>

**C32.** A Windows 10 application includes the installation of a service during the setup process. Which of the following would be the MOST important consideration during the application setup?

- A.** OS compatibility
  - B.** Available storage space
  - C.** Network connectivity
  - D.** User permissions
- 

**The Answer:** **D.** User permissions

A standard user account does not have permission to make significant operating system changes, especially those that would include the installation of a service. To prevent the unintended installation of malicious software, the Windows UAC (User Account Control) feature will request additional rights and permissions for these operating system changes.

**The incorrect answers:**

**A. OS compatibility**

Windows 10 applications tend to be compatible across all editions of Windows 10, so the compatibility of the software to the currently running operating system would not be the most significant consideration.

**B. Available storage space**

The installation of an application with a service does not generally have a significant storage requirement. The storage requirement would be about the same as an application that does not include the installation of a service.

**C. Network connectivity**

There's no mention of a network component to the application, so the current network status would not be the most important consideration for this installation.



**More information:**

220-1002, Objective 1.7 - Installing Applications

<https://professormesser.link/1002010701>

**C33.** A medical center requires that shared computer systems are installed in hallways and patient rooms for the hospital staff. However, hospital administrators are concerned that patient information might be visible if someone leaves the computer without logging out. Which of the following would help prevent this type of issue?

- A.** Multi-factor authentication
  - B.** Password expiration policy
  - C.** Login time restrictions
  - D.** Screensaver passwords
- 

**The Answer:** **D.** Screensaver passwords

Screensaver passwords would ensure that the information on the computer would be protected if someone walks away and leaves the system unattended. Other security enhancements might include a proximity monitor that would automatically lock the system when someone walks away, making the screensaver password a good secondary security option.

**The incorrect answers:**

**A.** Multi-factor authentication

Additional authentication factors would only provide security during the login process.

**B.** Password expiration policy

It's a good best practice to periodically require updated passwords, but those policies are not designed to protect a system that has been unlocked.

**C.** Login time restrictions

A login time restriction would prevent someone from authenticating at a certain time of the day. This type of restriction would not protect a system where the authentication has already occurred.



**More information:**

220-1002, Objective 2.7 - Workstation Security Best Practices

<https://professormesser.link/1002020701>

**C34.** George, a user, has a smartphone to assist with maps and directions when traveling to other company locations. At a remote site, George finds that his phone is attempting to contact a third-party website to share location information. Which of the following would be the BEST way to address this issue?

- A. Disable the GPS
  - B. Perform a soft reset
  - C. Run an anti-malware scan
  - D. Use the cellular network instead of Wi-Fi
- 

**The Answer:** C. Run an anti-malware scan

The symptom of the phone contacting a third-party website would commonly be associated with malware. None of the other options would provide any mitigation of the potential issue.

**The incorrect answers:**

**A. Disable the GPS**

Disabling the GPS might limit the scope of a potential malware infection because the malware would not have location information to share. However, this only addresses the symptom caused by the malware and not the problem of the malware itself.

**B. Perform a soft reset**

If this issue was related to malware, then a soft reset would not resolve the issue. Private information sent to a third-party is a significant security concern, so addressing the issue with an anti-malware scan is the best of the available options.

**D. Use the cellular network instead of Wi-Fi**

Changing the type of network used for the third-party communication would not limit or stop the sharing of location information.



#### More information:

220-1002, Objective 3.5

Troubleshooting Mobile Device Security

<https://professormesser.link/1002030501>

**C35.** A company requires all users to authenticate to a proxy before communicating to external websites. Which of the following should be used to integrate the proxy authentication with the existing Active Directory credentials?

- A.** WPS
  - B.** TKIP
  - C.** RADIUS
  - D.** WPA2
- 

**The Answer:** **C.** RADIUS

RADIUS (Remote Authentication Dial-in User Service) is an authentication protocol used to integrate with many existing user databases. It's common to use RADIUS to connect a service with an Active Directory database to use for centralized authentication.

**The incorrect answers:**

**A.** WPS

WPS (Wi-Fi Protected Setup) is a configuration method designed to simplify the connectivity to Wi-Fi networks. WPS will not integrate a third-party service with an Active Directory database.

**B.** TKIP

TKIP (Temporal Key Integrity Protocol) was commonly used with the original WPA (Wi-Fi Protected Access) encryption method on 802.11 wireless networks. WPA and TKIP are no longer recommended as encryption and integrity mechanisms.

**D.** WPA2

WPA2 (Wi-Fi Protected Access version 2) is an encryption technology for 802.11 wireless networks. WPA2 does not provide authentication integration to Active Directory databases.



**More information:**

220-1002, Objective 2.3 - Wireless Security  
<https://professormesser.link/1002020301>

**C36.** A desktop administrator has been tasked with removing malware from an executive's laptop computer. The system has been removed from the network, but the Windows startup process shows a Stop Error before rebooting into a repeating cycle. Which of the following would be the best NEXT step in the malware removal process?

- A. Perform a Windows Repair installation
  - B. Boot with a pre-installation environment
  - C. Schedule periodic scans
  - D. Create a restore point
- 

**The Answer:** B. Boot with a pre-installation environment

A Windows PE (Pre-installation Environment) can be used to boot into the Windows Recovery Console to help resolve problems with the primary operating system. This is a common task when the primary operating system has been corrupted or will not boot properly.

**The incorrect answers:**

**A. Perform a Windows Repair installation**

A Windows Repair installation may resolve the rebooting issue, but it may also make unintended changes to the operating system. Before making significant changes, it would be worthwhile to try fixing the issue manually.

**C. Schedule periodic scans**

Because the system is constantly rebooting, it's not possible to make configuration changes to the anti-virus scanner or the Task Scheduler.

**D. Create a restore point**

If a restore point already existed, it may be possible to reboot to a previous configuration. However, it would be too late to create a restore point with the existing faulty configuration.



**More information:**

220-1002, Objective 3.3 - Removing Malware  
<https://professormesser.link/1002030301>

**C37.** An audit has found that numerous email attachments include non-encrypted documents containing credit card numbers. A security administrator has been asked to prevent this information from being sent across the network. Which of the following would be the BEST way to provide this functionality?

- A.** Enable Windows Firewall
  - B.** Block all email at the Internet firewall
  - C.** Create a Group Policy
  - D.** Use a DLP solution
  - E.** Require multi-factor authentication
- 

**The Answer:** **D.** Use a DLP solution

A DLP (Data Loss Prevention) solution usually consists of hardware and software that monitors application and network traffic to prevent the loss of sensitive data. A DLP solution would prevent email messages containing credit card numbers from leaving the local protected network.

**The incorrect answers:**

**A.** Enable Windows Firewall

Windows Firewall does not include a method of detecting and blocking credit card numbers or other sensitive data.

**B.** Block all email at the Internet firewall

Blocking all email would be an aggressive policy that would certainly prevent credit card data from being transmitted over email, but it would also block legitimate email messages.

**C.** Create a Group Policy

Using Windows Group Policy can manage the use of the operating system, but it would not block sensitive information in email messages.

**E.** Require multi-factor authentication

Multi-factor authentication requires additional login credentials, but it does not prevent the transmission of sensitive information over email.



**More information:**

220-1002, Objective 2.2 - Logical Security

<https://professormesser.link/1002020201>

**C38.** A user has just upgraded a Windows application and has restarted their computer. Unfortunately, the Windows desktop no longer appears after the login process. Which of the following utilities would allow the system administrator to resolve this issue?

- A.** System Restore
  - B.** Performance Monitor
  - C.** bootrec
  - D.** Task Manager
  - E.** dxdiag
- 

**The Answer:** **A.** System Restore

The System Restore feature can roll back the Windows configuration to a previous date and time. Restore points are created automatically during an application install, so it would be relatively easy to revert back to the configuration before the upgrade.

**The incorrect answers:**

**B.** Performance Monitor

Performance Monitor displays long-term graphs and collects data regarding CPU, network, memory, and other system resources.

**C.** bootrec

The Windows bootrec (Boot Recovery) command is used to repair problems with the boot records, boot sectors, and the Boot Configuration Data (BCD).

**D.** Task Manager

The Windows Task Manager displays a real-time view of processes and their resource utilizations.

**E.** dxdiag

The dxdiag (DirectX Diagnostic) tool provide diagnostics of the system, display, sound, and input.



**More information:**

220-1002, Objective 1.5 - System Utilities

<https://professormesser.link/1002010506>

**C39.** A user in the shipping department is using a tracking app on a tablet. The app normally takes 10 seconds to load, but is now taking over a minute before it can be used. Tracking searches that normally take seconds are taking almost a minute to show the tracking details. Other tablets are not experiencing this slowdown. Which of the following would be the best NEXT troubleshooting step?

- A.** Reinstall the tracking app
  - B.** Check the app battery usage
  - C.** Roll back to the previous tablet OS version
  - D.** Perform a soft reset
- 

**The Answer:** **D.** Perform a soft reset

Before making any significant changes, a soft reset can be used to clear memory space and reset any potential conflicts.

**The incorrect answers:**

**A.** Reinstall the tracking app

Reinstalling the tracking app would make a change to the system. It would be much more efficient to reset the system and test before making any changes to the existing software.

**B.** Check the app battery usage

The performance of the app appeared to be related to performance on the network, and it did not appear that the battery usage was related to the issue.

**C.** Roll back to the previous tablet OS version

It would be useful to gather more troubleshooting information before making any significant system changes.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**C40.** Which of the following fire extinguishers would be most appropriate to use in a data center?

- A. Foam
  - B. Carbon Dioxide
  - C. Saline
  - D. Water
- 

**The Answer:** B. Carbon dioxide

A fire extinguisher that uses carbon dioxide, FM-200, or other dry chemicals would be the best choice for electronic equipment.

**The incorrect answers:**

**A.** Foam

The water-based foam extinguisher would not be a good choice for electrical equipment.

**C.** Saline

Any water-based extinguisher, especially one with salt, would be a very bad choice for a data center.

**D.** Water

Water is commonly used in fire extinguishers, but a data center and the large amount of powered electronics in a single room requires an extinguisher that can be used safely while it is putting out the fire.



**More information:**

220-1002, Objective 4.4 - Safety Procedures

<https://professormesser.link/1002040401>

**C41.** The Human Resources department is installing a shared computer in the company lobby to use for electronic job applications. The kiosk should start automatically without requiring any network login prompt, and the kiosk should only have access to the job application modules. Which of the following account types would be the BEST choice for this system?

- A. SSO user
  - B. Administrator
  - C. Guest
  - D. Power User
- 

**The Answer: C. Guest**

The Guest account is the only account that should be available on a public computer running applications for multiple users.

**The incorrect answers:**

**A. SSO user**

Windows does not include a user group for SSO (Single Sign-On) User, but if they did it would not be preferable over using the Guest account.

**B. Administrator**

The Administrator account provides complete access to the system and would be a poor choice for a public computer used by many different people.

**D. Power User**

The Power User group in Windows is now effectively the same as the standard user, but even that user would have more rights and permissions than necessary. The Guest account would be preferable to the Power User or standard user permissions.



**More information:**

220-1002, Objective 2.6 - Windows Security Settings

<https://professormesser.link/1002020601>

**C42.** An administrator needs to configure a COM+ application on the company's workstations. Which of the following should be used to complete this task?

- A. Device Manager
  - B. Local Security Policy
  - C. Component Services
  - D. Performance Monitor
- 

**The Answer:** C. Component Services

The Component Services Control Panel applet manages the configurations for Microsoft COM+ (Component Object Model) services.

**The incorrect answers:**

**A. Device Manager**

The Windows Device Manager is used to enable, disable, and configure hardware device drivers in the operating system.

**B. Local Security Policy**

The Local Security Policy applet can be used to configure password policies, account lockout policies, and other important security settings on the local operating system.

**D. Performance Monitor**

Performance Monitor gathers long-term statistics and performance metrics from the operating system. Performance monitor will not provide any configuration of COM+ applications.



**More information:**

220-1002, Objective 1.5 - Windows Administrative Tools

<https://professormesser.link/1002010501>

**C43.** A user in the shipping department is able to view order information, but they cannot modify or delete any order details. Which of the following would best describe this security principle?

- A.** Multi-factor authentication
  - B.** Least privilege
  - C.** Group Policy
  - D.** Data loss prevention
- 

**The Answer:** **B.** Least privilege

The principle of least privilege ensures that rights and permissions are set to the bare minimum to perform assigned duties. Users can only run applications within the scope of their job function, and application usage outside of that scope would be administratively prohibited.

**The incorrect answers:**

**A.** Multi-factor authentication

Multi-factor authentication provides additional login factors and does not affect the use of applications.

**C.** Group Policy

Group Policy is a configuration option associated with Active Directory networks that allows the administrator to manage the connected Windows devices. Group Policy is not a security principle associated with application rights and permissions.

**D.** Data loss prevention

Data loss prevention (DLP) is the process of identifying and preventing the loss of sensitive data. DLP solutions can identify sensitive data streams such as credit card numbers or social security numbers and block the transfer of the information through the network.



**More information:**

220-1002, Objective 2.2 - Logical Security

<https://professormesser.link/1002020201>

**C44.** A user has just completed the installation of a new video driver on their Windows 10 laptop and has rebooted the system. Instead of the Windows login screen, the laptop shows a black screen with no additional information or messages. Which of the following would be the best NEXT troubleshooting step?

- A. Update the BIOS
  - B. Modify the BCD settings
  - C. Start in VGA mode
  - D. Update to the latest OS patches
- 

**The Answer:** C. Start in VGA mode

Starting in VGA mode from the Advanced Startup Options will launch Windows with the generic VGA drivers. If a change to a video driver or display causes a black screen, the generic VGA mode may allow access to the desktop and future troubleshooting options.

**The incorrect answers:**

**A. Update the BIOS**

Making a change to the BIOS would not resolve a black screen issue after upgrading a video driver.

**B. Modify the BCD settings**

The BCD (Boot Configuration Data) would need to be updated if the system did not locate a Windows operating system to boot. In that situation, a message would be displayed that states "An operating system wasn't found."

**D. Update to the latest OS patches**

The operating system would not need to be patched because a video driver was updated. Before making any additional operating system changes, it would be best to troubleshoot the current issue.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Windows  
<https://professormesser.link/1002030101>

**C45.** A small office is located in a large office building that contains over fifty different companies. A network administrator would like to limit the possibility of someone else in the building accidentally connecting to their wireless network. Which of these configuration settings would prevent their wireless network from appearing in a list of available networks?

- A.** MAC filtering
  - B.** Static IP addressing
  - C.** WPA2 encryption
  - D.** SSID suppression
- 

**The Answer:** **D.** SSID suppression

SSID (Service Set Identifier) suppression will prevent the wireless network name from appearing in lists of available networks. Users who know the name can still connect to the network manually.

**The incorrect answers:**

**A.** MAC filtering

MAC (Media Access Control) filtering can be configured to restrict or allow specific wireless devices when accessing the network. MAC filtering does not remove the name of the wireless network from the availability list.

**B.** Static IP addressing

Static IP addressing will change the addressing on the devices connected to the wireless network, but it won't remove the name of the network from the list of available wireless connections.

**C.** WPA2 encryption

WPA2 (Wi-Fi Protected Access version 2) is a security protocol included on 802.11 wireless networks. Enabling WPA2 does not remove the name of the wireless network from the list of available connections.



**More information:**

220-1002, Objective 2.10 - Securing a SOHO Network  
<https://professormesser.link/1002021001>

**C46.** A manager in the accounting department would like to upgrade to Windows 10, but she doesn't want to lose access to any of the currently installed applications or data. Which of the following methods would be the BEST choice for these requirements?

- A.** Clean install
  - B.** Unattended installation
  - C.** Network installation
  - D.** In-place upgrade
- 

**The Answer:** **D.** In-place upgrade

An in-place upgrade keeps all of the existing data, applications, and configurations in place during the upgrade process.

**The incorrect answers:**

**A.** Clean install

A clean install removes all previous data from a system. After a clean install is complete, the user would need to restore their data files from backup and reinstall all of their applications.

**B.** Unattended installation

An unattended installation might be useful for an automated upgrade, but an unattended installation doesn't necessarily mean that the process is an in-place upgrade.

**C.** Network installation

An installation occurring over the network is often done to simplify the process and avoid the need for each workstation to use boot media. A network installation doesn't necessarily mean that an in-place upgrade is occurring.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**C47.** A network administrator has modified all wireless access points to use WPA2 instead of WEP. Which of the following would be the main reason for this change?

- A.** Faster throughput
  - B.** Better reception and range
  - C.** Reduced power use
  - D.** Better security
- 

**The Answer: D. Better Security**

WEP (Wired Equivalent Privacy) is the original security technology used on 802.11 wireless networks. Significant cryptographic vulnerabilities were found in WEP, and the industry eventually created the much more secure WPA2 (Wi-Fi Protected Access version 2) security technology to replace it.

**The incorrect answers:**

**A.** Faster throughput

The throughput differences between WEP and WPA2 are negligible, and throughput would not be the primary reason for making this change.

**B.** Better reception and range

Neither WEP nor WPA2 are related to the radio frequency output and range of the wireless signal.

**C.** Reduced power use

Both WEP and WPA2 are similar technologies and neither has a significant power usage difference over the other.



**More information:**

220-1002, Objective 2.3 - Wireless Security

<https://professormesser.link/1002020301>

**C48.** A help desk is receiving reports that a group of devices is not able to communicate outside of their local IP subnet. A technician can ping devices on the same network, but does not receive a response when pinging the IP address of external devices. Which of the following would be the MOST likely cause of this issue?

- A. Default gateway
  - B. DNS server
  - C. Proxy server
  - D. QoS
- 

**The Answer:** A. Default gateway

The default gateway is the router that provides the communication between the local IP subnet and the rest of the world. If the default gateway isn't working, users will not be able to access services that are outside of the local subnet.

**The incorrect answers:**

**B. DNS server**

The DNS server converts between a fully qualified domain name and an IP address. In this example, the technician was attempting to ping external devices by IP address, so the DNS server would not be part of this issue.

**C. Proxy server**

A proxy server is commonly used to provide security for incoming or outgoing web services. A technician pinging an external IP address would not commonly be communicating through a proxy server.

**D. QoS**

QoS (Quality of Service) is a technology that can prioritize different traffic flows on the network. Although QoS can control some traffic, it would not be common for QoS to prevent all traffic from passing through the network.



**More information:**

220-1002, Objective 1.8 - Windows IP Address Configuration  
<https://professormesser.link/1002010805>

**C49.** A network technician has been tasked with preventing corporate laptops from connecting to a training room's wireless network. Which of the following would be the BEST way to accomplish this?

- A.** Enable MAC filtering
  - B.** Use WPS
  - C.** Apply static IP addressing
  - D.** Create content filters
- 

**The Answer:** **A.** Enable MAC filtering

MAC (Media Access Control) filtering will control access to a network based on the physical MAC address of the device. In this scenario, the technician can create a MAC filter that will allow all of the training room devices and block all other addresses.

**The incorrect answers:**

**B.** Use WPS

WPS (Wi-Fi Protected Setup) allows users to easily connect to wireless networks without having to configure detailed security settings. Enabling WPS on a wireless router would not prevent users from connecting to the network.

**C.** Apply static IP addressing

Static IP addressing requires the administrator to manually configure IP addressing on each device. However, this process does not restrict a user from initially connecting to the wireless network.

**D.** Create content filters

Content filtering is commonly used to restrict traffic based on data within the content, such as inappropriate web sites or other sensitive materials.



**More information:**

220-1002, Objective 2.10 - Securing a SOHO Network

<https://professormesser.link/1002021001>

**C50.** While working at a customer's desk, a technician's mobile phone begins to ring. Which of the following would be the MOST appropriate response?

- A. Take the call and address the caller's requests before continuing
  - B. Take the call and ask the caller if you can return their call later
  - C. Send the call to voicemail and apologize for the interruption
  - D. Politely excuse yourself and step out to take the call
- 

**The Answer:** C. Send the call to voicemail and apologize for the interruption  
When actively working on a problem with a customer, it's important to avoid interruptions, distractions, and anything else that would change focus from the current task.

**The incorrect answers:**

**A.** Take the call and address the caller's requests before continuing  
It would be unprofessional to allow a phone call to interrupt the current troubleshooting tasks. All calls should be sent to voice mail and can be returned after the customer interaction is complete.

**B.** Take the call and ask the caller if you can return their call later  
It's not necessary to take a phone call to simply tell the caller that they will receive a return call. Instead of interrupting the current customer interaction, it's more professional to send the calls to voice mail.

**D.** Politely excuse yourself and step out to take the call  
The primary focus of a customer visit is to solve the customer's problems and not to take calls from others. It would be more professional to send the call to voice mail and continue working on the current task.



**More information:**

220-1002, Objective 4.7 - Professionalism  
<https://professormesser.link/1002040702>

**C51.** A user's workstation has been identified as participating in a DDoS to a large Internet service provider. The computer has been powered down and stored in a locked area until investigators arrive. Which of these procedures would be the MOST important to follow in the meantime?

- A.** Create documentation of the storage area
  - B.** Retrieve logs from the workstation Event Viewer
  - C.** Obtain the purchase records of the workstation
  - D.** Maintain integrity of the workstation data
- 

**The Answer:** **D.** Maintain integrity of the workstation data

When a security event occurs, it's important to maintain the integrity of the evidence and create a chain of custody. The data currently stored on the workstation should not be modified in any way.

**The incorrect answers:**

**A.** Create documentation of the storage area

Documenting the storage area would not be the most important part of the incident response process. If documentation is needed later, it can be created at that time.

**B.** Retrieve logs from the workstation Event Viewer

The workstation has been powered off and locked away to avoid changing any data on the storage drives. Starting the system to retrieve the logs would modify information on the storage drives.

**C.** Obtain the purchase records of the workstation

The purchase records of the workstation are not the most important piece of information for this security event. If the records are required later, they can be retrieved at that time.



**More information:**

220-1002, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1002040601>

**C52.** A system administrator has configured EFS on a user's workstation. Which of the following would describe this functionality?

- A.** Encryption of individual files and folders
  - B.** Conservation of bandwidth to remote sites
  - C.** Encrypted network tunnel
  - D.** Full disk encryption
- 

**The Answer:** **A.** Encryption of individual files and folders

EFS (Encrypting File System) is a feature of NTFS (NT File System) to encrypt individual files and folders on a drive without encrypting other parts of the file system.

**The incorrect answers:**

**B.** Conservation of bandwidth to remote sites

Enterprise editions of Windows 10 include the BranchCache feature. BranchCache can be used to cache commonly used files at remote sites instead of constantly transmitting those files across slower WAN links.

**C.** Encrypted network tunnel

A VPN (Virtual Private Network) would be a commonly used encryption method for network communication. EFS does not include any encryption for network communication.

**D.** Full disk encryption

BitLocker is the Windows option for full disk encryption. BitLocker encrypts entire volumes, and EFS is used to encrypt individual files and folders.



**More information:**

220-1002, Objective 1.2 - Windows in the Enterprise  
<https://professormesser.link/1002010204>

**C53.** An application update has been installed to all computers in the accounting department. Sam, a user, starts the updated application for the first time but nothing appears on the screen. Which of the following would be the best NEXT troubleshooting step?

- A.** Reinstall the application
  - B.** Add Sam to the Administrator's group
  - C.** Install the latest Windows updates
  - D.** Check the Event Viewer
- 

**The Answer:** **D.** Check the Event Viewer

The Windows Event Viewer maintains a log of all system and applications processes. If an error occurs in an application, it's very likely that detailed information can be found in the Event Viewer logs.

**The incorrect answers:**

**A.** Reinstall the application

There's no evidence that the problem is associated with a bad application installation. Before making any changes to the application files, it would be useful to learn more about the root cause of the problem.

**B.** Add Sam to the Administrator's group

As a best practice, there is never a case where a user should be added to the Administrator group. User applications do not need Administrator access, and assigning this access can introduce significant security issues.

**C.** Install the latest Windows updates

Since the root cause of the issue has not been determined, making changes to the application or the operating system would not be the best next step. Once more information is known about the problem, a Windows update may be necessary. Until then, it's best to gather as much information as possible about the problem.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues  
<https://professormesser.link/1002030201>

**C54.** A technician has been asked to work on an urgent computer repair while the user is at lunch. When the technician arrives, they notice paperwork on the desk that may contain private customer information. Which of the following would be the BEST next step?

- A. Complete the repair as quickly as possible
  - B. Ask an associate in the department for assistance
  - C. Move the papers somewhere out of sight
  - D. Leave without repairing the computer
- 

**The Answer:** B. Ask an associate in the department for assistance

The technician has a job to complete, but privacy and access to sensitive information is an important consideration. In these situations, it's best to work with others to remove any of these concerns from the work area.

**The incorrect answers:**

A. Complete the repair as quickly as possible

The issue with this repair isn't about how quickly the job can be completed, but more about the type of data the technician can see. To avoid any issues, it would be best to have a trusted third-party remove the sensitive information from the area.

C. Move the papers somewhere out of sight

Moving any papers, especially papers containing sensitive information, would not be a good idea. If the technician touches the papers, then they effectively have access to all of the information on the documents. A third-party in the department can move things to create a proper work environment for the repair.

D. Leave without repairing the computer

The user would prefer that their computer repair was completed, and the technician is already on-site and at their desk. Asking someone else in the department to clean the work area would only take a moment and would allow the repair process to continue.



**More information:**

220-1002, Objective 4.7 - Professionalism

<https://professormesser.link/1002040702>

**C55.** A company has recently been the victim of a storm with large-scale flooding, and all systems and backups at the corporate data center were completely destroyed. Which of the following would be the BEST way to avoid this loss of data in the future?

- A.** Uninterruptible power supplies
  - B.** Cloud storage
  - C.** RADIUS administration servers
  - D.** Image-level backups
- 

**The Answer:** **B.** Cloud storage

Cloud storage would provide a separate, off-site storage of backups, files, and other important documents. One significant advantage of any off-site backup or storage is to have access to the data if the primary site was to have any type of disaster.

**The incorrect answers:**

**A.** Uninterruptible power supplies

An uninterruptible power supply (UPS) would provide a backup power source if the primary power was to become unavailable. A UPS would not provide any method of data backup or data recovery.

**C.** RADIUS administration servers

RADIUS (Remote Authentication Dial-In User Service) servers provide a method to authenticate login processes to a centralized user database. In the case of a disaster, users would still be able to login to their important services using these authentication technologies. RADIUS does not provide any data backup or data recovery features, however.

**D.** Image-level backups

An image-level backup can be an important part of a backup strategy, but simply performing the image-level backup won't be helpful if the backup services are destroyed during a natural disaster. In this example, having an off-site backup data source would have prevented the data loss.



**More information:**

220-1002, Objective 4.3 - Disaster Recovery

<https://professormesser.link/1002040301>

**C56.** A user commonly stores large graphic image files in a shared folder on a network server. After logging in one morning, the user notices that the shared folders are no longer in the list of available storage drives. The user confirms that they are logged in properly to the Windows Domain. Which of the following would be the MOST likely reason for this issue?

- A.** User's permissions have been modified
  - B.** User is running untrusted software
  - C.** Network is using MAC filtering
  - D.** Port security is enabled
- 

**The Answer:** **A.** User's permissions have been modified

The login process and Windows desktop are working normally without any identified errors, so the operating system is most likely working normally. Since the normal list of shares has changed, then it's most likely that something has been modified with the share permissions.

**The incorrect answers:**

**B.** User is running untrusted software

Untrusted software can be managed in many different ways, but a share not appearing in a list is not commonly associated with an application. The display of the share is managed by the operating system, so this issue would most likely be associated with a permission change or problem.

**C.** Network is using MAC filtering

MAC (Media Access Control) filtering allows or prevents a device from communicating on a network. MAC filtering is not used to limit or restrict access to a particular Windows share.

**D.** Port security is enabled

Port security allows the network administrator to provide access to the network based on a user's login credentials. Port security is not used to limit access to a Windows share.



**More information:**

220-1002, Objective 2.2 - Logical Security

<https://professormesser.link/1002020201>

**C57.** A company deploys a suite of commercial software onto every workstation in the organization. Which of the following would BEST describe this licensing?

- A.** Personal licenses
  - B.** Enterprise license
  - C.** FOSS license
  - D.** End user licensing agreement
- 

**The Answer:** **B.** Enterprise license

An enterprise software license is commonly used for large-scale licensing of software, and often covers every device on the organization's network.

**The incorrect answers:**

**A.** Personal licenses

A personal license is usually associated with an individual or home-based use of software. Individual personal licenses might be appropriate for smaller groups of users, but larger licensing agreements are required when purchasing for an entire organization.

**C.** FOSS license

A FOSS (Free and Open-Source Software) license does not require any payment, so there isn't usually a commercial component or financial arrangement associated with the use of FOSS licensing.

**D.** End user licensing agreement

An end user licensing agreement (EULA) is a list of the licensing terms associated with the use of software. A EULA can be associated with enterprise licenses, personal licenses, and FOSS licenses.



**More information:**

220-1002, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1002040601>

**C58.** A desktop administrator is troubleshooting an issue with a client's desktop computer that dual-boots between Windows and Linux. Due to a change in job requirements, the Linux operating system was removed from the desktop computer. Now when the computer is powered on, Windows does not start and the computer displays the message, "Missing operating system." The administrator has confirmed that the storage drive is operating properly, and when they boot with a Windows Preinstallation Environment they can see the user's data on the drive. Which of the following would be the BEST way to resolve this issue?

- A.** Modify the boot order in the BIOS
  - B.** Reinstall the Windows operating system
  - C.** Boot to Safe Mode and disable all startup applications
  - D.** Reinstall the Windows boot manager
- 

**The Answer:** **D.** Reinstall the Windows boot manager

When removing operating systems from a dual-boot system, the Windows boot manager may not be referenced during startup. The bootrec command in the Recovery Console can correct this issue and allow the system to start normally.

**The incorrect answers:**

**A.** Modify the boot order in the BIOS

The system is already booting from the correct drive. Modifying the boot order would not resolve this issue.

**B.** Reinstall the Windows operating system

The user's Windows data is still on the drive, so reinstalling Windows would not be the best way to resolve this boot issue.

**C.** Boot to Safe Mode and disable all startup applications

The system will not boot into the normal Windows desktop. It's unlikely that it would be able to boot into Safe Mode.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1002030101>

**C59.** A user is working with a .dmg file on their macOS desktop. Which of the following would describe the contents of this file?

- A.** Debug information
  - B.** Disk image
  - C.** Application library
  - D.** Disk maintenance utility
- 

**The Answer:** **B.** Disk image

The macOS equivalent to an ISO file is a DMG (Disk Image) file. Disk images can be created and managed from the macOS Disk Utility.

**The incorrect answers:**

**A.** Debug information

Debug information is commonly available in the macOS console or directly from an application. A .dmg file is not a container of debug information.

**C.** Application library

Application library files in macOS are used to contain back-end configurations, framework classes, and other important application files. These files are often stored in the Library folder in macOS. The .dmg file is not used to store application library files.

**D.** Disk maintenance utility

The macOS Disk Utility can be used to create and manage .dmg files, but the disk maintenance utility would not necessarily be contained within a .dmg file.



**More information:**

220-1002, Objective 1.9 - macOS Tools

<https://professormesser.link/1002010902>

**C60.** A member of the accounting department at headquarters is getting a new laptop and would like to reissue the older Windows 10 laptop to an accounting team member at a remote site. The headquarters user would like to remove all personal files, apps, and settings before sending the laptop to the remote site. Which of the following would be the BEST way to accomplish this?

- A. Remove the Windows partition and reinstall
  - B. Perform a Windows 10 reset
  - C. Perform a secure wipe and reinstall from original Windows media
  - D. Uninstall all apps under Control Panel / Programs and Features
- 

**The Answer:** B. Perform a Windows 10 reset

Of the available options, the Windows 10 reset can quickly remove all personal files, apps, and setting, and would reset the system to the factory defaults.

**The incorrect answers:**

A. Remove the Windows partition and reinstall

Removing the Windows partition and reinstalling the entire operating system would certainly remove all of the previous owner's content, but it would take longer and accomplish the same task as a Windows 10 reset.

C. Perform a secure wipe and reinstall from original Windows media

Since this device is being used in the same department of the same company, a secure wipe would not be a common requirement and it wasn't mentioned as part of the question. A much faster deployment method would be to use the Windows 10 reset feature.

D. Uninstall all apps under Control Panel / Programs and Features

Uninstalling with the Control Panel applet would be a very slow method of removing applications, and it wouldn't remove personal files and configurations.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Solutions

<https://professormesser.link/1002030102>

**C61.** Walter, a user, has noticed that his computer begins to slow down during daily use and eventually locks up completely. During the lock up, the keyboard and mouse do not respond and the screen does not show any error messages. Which of the following tasks should a technician follow to BEST troubleshoot this issue? (Choose TWO)

- A. Start the computer in Safe Mode
  - B. Perform a hardware diagnostic
  - C. Connect the computer to a different VLAN
  - D. Update the OS to the latest patches
  - E. Roll back to a previous configuration
  - F. Scan for viruses and malware
- 

**The Answer:** **B.** Perform a hardware diagnostic, and **F.** Scan for viruses and malware

Without knowing the root cause of the issue, it will be important to gather as much information about the issue without making any changes to the operating system or applications. A hardware diagnostic would provide information about the health of the computer equipment, and scanning for viruses would check for any malicious software. Neither of those options would make any changes to the configuration of the system.

**The incorrect answers:**

**A.** Start the computer in Safe Mode

Since this issue occurs over time, simply starting the computer in Safe Mode would not provide much information about the issue.

**C.** Connect the computer to a different VLAN

The issue does not appear to be related to network connectivity, so choosing a different VLAN for this computer would most likely not result in any change. VLAN assignments don't tend to slow computers down over time, so this would also not be a common solution to the issue.

**D. Update the OS to the latest patches**

Before making any changes to the operating system, it would be more important to gather information and test components without changing application or operating system files.

**E. Roll back to a previous configuration**

There's no evidence that the current issue is related to a specific changes, so rolling back to a previous configuration would not be the best of the available options. This option would also make changes to the existing configuration before understanding what the root cause might be.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues

<https://professormesser.link/1002030201>

**C62.** A user receives this message each time they visit a secure website: “The site’s security certificate is not trusted.” A technician investigates the issue and finds that the problem only occurs on this user’s computer and not with other computers in the same office. Which of the following would be the best NEXT troubleshooting task?

- A. Disable Windows Firewall for all HTTPS traffic
  - B. Create a new certificate for the user’s computer
  - C. Check the date and time on the user’s computer
  - D. Release and refresh the IP address configuration
- 

**The Answer:** C. Check the date and time on the user’s computer

The message regarding the site’s security certificate is shown because the local computer can’t validate the certificate on the web server. The server’s certificate has a specific issuing and expiration date and time, so an incorrect date and time on the workstation could cause the validation to fail on the workstation.

**The incorrect answers:**

A. Disable Windows Firewall for all HTTPS traffic

HTTPS (Hypertext Transfer Protocol Secure) is a secure protocol used for encrypted communication to a website. Disabling the firewall for HTTPS traffic will not change the validation process of a web site certificate.

B. Create a new certificate for the user’s computer

The certificate failing the validation is located on the web server. Creating or changing a certificate on the user’s computer will have no effect on the web site certificate validation.

D. Release and refresh the IP address configuration

The issue with trusting a website certificate is not related to the IP address of the workstation. Changing or refreshing the dynamic IP address assignment will not change the certificate validation process.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues

<https://professormesser.link/1002030201>

**C63.** A user's smartphone contains company confidential information that should not be shared outside of the organization. Which of the following would be the BEST way to limit access to this data if the smartphone was lost or stolen?

- A. PIN
  - B. Remote wipe
  - C. Swipe pattern
  - D. Cloud backup
- 

**The Answer:** B. Remote wipe

The remote wipe feature of a smartphone or tablet allows the administrator or owner of the device to delete all information on the device from a website or secure app. If the device is lost or stolen, all of the data on the device can be immediately erased and recovery of the data would not be possible.

**The incorrect answers:**

**A. PIN**

A PIN (Personal Identification Number) can be used as an authentication factor when unlocking the smartphone. The PIN feature would not be the best way to limit access to the data if the device is lost or stolen.

**C. Swipe pattern**

The swipe pattern is another lock screen authentication factor that uses a known pattern to provide access to the smartphone contents. The swipe pattern would not be the best way to limit access to the smartphone data.

**D. Cloud backup**

A cloud backup allows the smartphone owner to recover data if the phone were lost or stolen, but the cloud backup would not provide any additional protection of the smartphone data.



**More information:**

220-1002, Objective 2.8 - Securing Mobile Devices  
<https://professormesser.link/1002020801>

**C64.** An IT organization has created a series of Windows 10 file share names that end with a dollar sign (\$). Which of the following would describe these shares?

- A. Optimized
  - B. Hidden
  - C. Remote
  - D. Encrypted
- 

**The Answer:** B. Hidden

The dollar sign symbol appended to a share name will hide that share from any lists or view commands. This is intended to be an administrative feature and not a security feature. Users who already know the share name can still connect and use the Windows share if they have the correct permissions.

**The incorrect answers:**

**A. Optimized**

Using a dollar sign in a Windows share does not enable any optimization features. The dollar sign is only used to hide the share from any populated lists or the net view command.

**C. Remote**

Technically speaking, most Windows shares are on a remote device. A dollar sign in the share name does not provide any information about the location of the share and the local device.

**D. Encrypted**

Information stored in a file system can be encrypted by default, but the name of a share does not determine if the data is on an encrypted volume. The dollar sign is only used for visibility of the share name.



**More information:**

220-1002, Objective 1.8 - Windows Network Technologies

<https://professormesser.link/1002010802>

**C65.** A computer on a manufacturing floor has a virus, and the system administrator has removed the system from the company network. Which of the following virus removal tasks should occur NEXT?

- A.** Discuss virus prevention with the end user
  - B.** Install the latest anti-virus signatures
  - C.** Schedule a virus scan to run each morning
  - D.** Disable System Restore
- 

**The Answer:** **D.** Disable System Restore

Before making any updates or changes to the system, it's important to remove any potentially infected restore points by disabling the System Restore feature.

**The incorrect answers:**

**A.** Discuss virus prevention with the end user

Talking to the end user about ways to prevent malware infections in the future should be the last step in the malware removal phase. The steps prior to end user education should focus on identification and removal of the malware.

**B.** Install the latest anti-virus signatures

Before installing updated signatures and beginning the mitigation phase, it's important to disable System Restore so the restore points won't be used to accidentally reinfect the system.

**C.** Schedule a virus scan to run each morning

After the malware is removed, the system administrator should verify that real-time malware detection is enabled and a schedule is in place to download the latest signatures and perform a full system scan.



**More information:**

220-1002, Objective 3.3 - Removing Malware

<https://professormesser.link/1002030301>

**C66.** A user in the marketing department needs to move data between macOS and Windows computers using a USB flash drive. Which of the following file systems would be the BEST way to easily transfer files between these operating systems?

- A.** exFAT
  - B.** HFS+
  - C.** NTFS
  - D.** NFS
- 

**The Answer:** **A.** exFAT

The exFAT (Extended File Allocation Table) file system is designed for flash drives and can be used across Windows, Linux, macOS, and other operating systems.

**The incorrect answers:**

**B.** HFS+

HFS+ (Hierarchical File system Plus) is a macOS file system. HFS+ is not compatible with Windows and would not be the best choice when transferring files between systems.

**C.** NTFS

The NTFS (NT File System) file system is the standard for Windows devices. Although it can be read by macOS, it is not completely compatible with the macOS operating system.

**D.** NFS

NFS (Network File System) is a method of accessing files across the network as if they were local. NFS is not used for transferring files with a USB flash drive.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**C67.** When a user starts their desktop computer, the Windows splash screen is shown with a rotating circle, but the login screen is never displayed. A technician researches the issue and finds that the computer was just updated to the latest set of Windows patches. Which of the following would be the NEXT step the technician should follow to help solve this issue?

- A. Reconfigure the BCD settings
  - B. Perform a Startup Repair
  - C. Start in VGA mode
  - D. Rebuild the user's profile
- 

**The Answer:** B. Perform a Startup Repair

The Windows Startup Repair is an automated feature that will examine each phase of the startup process and reconfigure any invalid or incorrect settings. This is a common repair to use when the startup process is not working properly after an application or operating system update.

**The incorrect answers:**

**A. Reconfigure the BCD settings**

The BCD (Boot Configuration Data) settings are used to locate and boot Windows. If the Windows splash screen is appearing, then the system was able to properly start the operating system and a reconfiguration of the BCD settings would not be necessary.

**C. Start in VGA mode**

If Windows was displaying a completely black screen instead of the login prompt, then starting in VGA mode may be useful. In this example, the Windows splash screen and rotating circle were visible on the screen.

**D. Rebuild the user's profile**

A bad user profile might cause the desktop to appear differently than normal and user files may not be visible from the File Explorer. In this example, the desktop and other user files were not accessible because the login prompt did not appear.



**More information:**

220-1002, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1002030101>

**C68.** A desktop technician is moving hard drives from one set of training room computers to another. Which of the following would allow the drives to be used in the new computers but prevent any of the existing data from being recovered?

- A.** Shredder
  - B.** Quick format
  - C.** Drill
  - D.** Standard format
- 

**The Answer:** **D.** Standard format

The Windows standard format will overwrite each sector of the drive, which will prevent any recovery tools from restoring any of the previous data.

**The incorrect answers:**

**A.** Shredder

A shredder will physically cut the drive into small pieces. This certainly prevents the recovery of the data, but it also causes the drive to be permanently damaged and unusable.

**B.** Quick format

A Windows quick format overwrites the file system table and marks all of the data on the drive as "deleted." None of the sectors are overwritten, and recovery software will be able to restore the remaining data.

**C.** Drill

A drill will ensure that the data cannot be recovered, but it physically damages the drive so that it cannot be used by others.



**More information:**

220-1002, Objective 2.9 - Data Destruction and Disposal

<https://professormesser.link/1002020901>

**C69.** A workstation technician manages a training center that contains thirty student computers in each room. All of the computers have the same hardware configurations. Which of these installation methods would be the BEST choice for quickly resetting the training rooms at the end of each week?

- A. In-place upgrade
  - B. Image installation
  - C. Repair installation
  - D. Clean install
- 

**The Answer:** B. Image installation

An image installation can install an operating system, applications, and customized system configurations to multiple devices in a single step. With a pre-built images, a large training room of systems can be updated with a specific configuration very efficiently.

**The incorrect answers:**

**A. In-place upgrade**

An in-place upgrade will modify the version of Windows running on a system. In this example, the systems need to be reset to their original state.

**C. Repair installation**

A repair installation is used to fix an installation that cannot boot properly to a Windows desktop. The repair installation will attempt to repair portions of the startup process, but it will not modify the user's files or applications.

**D. Clean install**

A clean install would provide a fresh starting point, but it doesn't include any of the applications required for the training facility. Most systems will require additional configurations and application installations after a clean install.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**C70.** A user has asked a technician to repair the display on a smartphone that works normally every morning but is very dim in the afternoon. The technician has performed a soft reset but the display is still dim. Which of the following would be the MOST likely reason for this issue?

- A.** Power saving mode
  - B.** Corrupted OS update
  - C.** Non-working backlight
  - D.** The battery is charging
- 

**The Answer:** **A.** Power saving mode

The power saving mode in a smartphone or tablet can be configured to dim the screen and disable certain features that use the battery. The backlight of the screen is one of the larger battery drains, so dimming the screen will help with the conservation process.

**The incorrect answers:**

**B.** Corrupted OS update

A corrupted operating system would might cause the system to hang or display an error message, but it would not be common for a corrupted operating system to modify the status of the backlight over time.

**C.** Non-working backlight

If the backlight had failed, then the display would barely be visible and would not be usable in the morning or afternoon. The screen on a system with a failed backlight would always be very dim and difficult to see.

**D.** The battery is charging

The battery on a smartphone can charge and display the screen at its highest brightness at the same time. It would not be normal for the charging process to cause the screen to become dimmer.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps  
<https://professormesser.link/1002030401>

**C71.** A desktop technician is troubleshooting a user's laptop with very high utilization, even with no activity on the screen or user input to the operating system. Task Manager shows that the CPU is operating at 100% utilization, memory utilization is slightly elevated, and there is a large amount of outbound network communication. Which of the following would be the MOST likely reason for these issues?

- A. System RAM is faulty
  - B. User has not properly authenticated
  - C. Laptop is part of a botnet
  - D. Network adapter is faulty
- 

**The Answer:** C. Laptop is part of a botnet

High CPU utilization, memory use, and network traffic with no user intervention indicates a possible malware infection and participation in a botnet. Of the available options, this would be the most likely reason for these symptoms.

**The incorrect answers:**

**A. System RAM is faulty**

Bad system memory usually causes the system to fail with a Windows stop error or to simply hang. Bad system RAM would not cause the CPU, memory, or network issues on this user's laptop.

**B. User has not properly authenticated**

A user who has not authenticated would be expected to have less CPU, memory, and network resource usage. It would not be common for an authentication issue to cause this resource activity.

**D. Network adapter is faulty**

A bad network adapter might cause errors to accumulate on the network link, but it would not commonly cause an increase in CPU and memory usage.



**More information:**

220-1002, Objective 2.4 - Types of Malware

<https://professormesser.link/1002020401>

**C72.** Daniel, a user in the marketing department, has been notified that other users have received email messages that show him as the sender, but he did not send the emails. There are no records of these emails in Daniel's sent messages folder. A technician researching the issue finds that Daniel's computer appears to be working properly and is not infected with any malicious software. Which of these should the technician check NEXT?

- A.** Email hijacking
  - B.** Invalid email certificate
  - C.** VLAN mismatch
  - D.** Incorrect email server configuration
- 

**The Answer:** **A.** Email hijacking

In this example, it does not appear that Daniel's workstation is sending the email messages from the email server. If an attacker has obtained Daniel's email username and password, they can send messages directly from the email server with his credentials.

**The incorrect answers:**

**B.** Invalid email certificate

An invalid email certificate would cause problems with encryption, decryption, and digital signatures. An invalid certificate would not cause messages to be sent from user without any user intervention.

**C.** VLAN mismatch

A VLAN mismatch would cause a device to appear on a different IP subnet, but it would not cause email messages to be sent without any user intervention.

**D.** Incorrect email server configuration

An incorrect email server configuration would cause the user's email client to show error messages and would fail to send or receive messages from the email server. An incorrect email server configuration would not cause messages to be sent without any user intervention.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues

<https://professormesser.link/1002030201>

**C73.** A company has created an internal process to ensure that all PII is encrypted. Which of the following would be the MOST likely reason for adding this additional security?

- A.** Helps prevent identity theft
  - B.** Improves application performance
  - C.** Allows customer data to be easily deleted
  - D.** Uses less storage space
- 

**The Answer:** **A.** Helps prevent identity theft

PII (Personally Identifiable Information) is any information that can identify an individual, such as an address, phone number, or date of birth. Encrypting PII will help prevent the unintended release of personal data and would assist with preventing identity theft.

**The incorrect answers:**

**B.** Improves application performance

The process of encrypting and decrypting data adds more overhead to the data storage process. Although application performance may not become any worse, the encryption process would not commonly increase performance.

**C.** Allows customer data to be easily deleted

The removal of customer data is not made easier through the use of encryption. Although it's useful to have processes to remove user information, that process is managed in conjunction with the encryption and decryption process.

**D.** Uses less storage space

The encryption process would not commonly be used as a way to decrease the use of storage space. If encryption and decryption is being used, then there is most likely a security focus for implementing such a process.



**More information:**

220-1002, Objective 4.6 - Privacy, Licensing, and Policies  
<https://professormesser.link/1002040601>

**C74.** A system administrator is installing a file server into the corporate data center. Which of the following would be the BEST way to improve security of the file sharing service? (Select TWO)

- A. Enable a BIOS user password
  - B. Connect the server to a wireless network
  - C. Limit the number of concurrent connections
  - D. Disable unused accounts
  - E. Enable file storage quotas
  - F. Enable password complexity
- 

**The Answers:** D. Disable unused accounts, and  
F. Enable password complexity

The only available options associated with server security are those to disable unused accounts and increase the complexity of the passwords. Unused accounts can be exploited, and passwords that are easy to guess or set to defaults can be discovered by an attacker.

**The incorrect answers:**

A. Enable a BIOS user password

Enabling a password during the startup process does not protect the server once it has started.

B. Connect the server to a wireless network

Wireless networks do not provide any additional application security. Connecting to a wireless network would not improve the security posture of the server.

C. Limit the number of concurrent connections

Limiting concurrent connections would restrict the throughput of the service and would not provide any security enhancements.

E. Enable file storage quotas

Storage quotas would conserve storage space on the server, but they would not provide any additional security enhancements.



**More information:**

220-1002, Objective 2.7 - Workstation Security Best Practices

<https://professormesser.link/1002020701>

**C75.** A user has purchased a computer that uses a 32-bit version of an operating system. Which of the following would be the maximum amount of RAM supported in this OS?

- A. 32 GB
  - B. 2 TB
  - C. 512 GB
  - D. 128 GB
  - E. 4 GB
  - F. 16 GB
- 

**The Answer:** E. 4 GB

A 32-bit operating system can store  $2^{32}$  values, or approximately 4 GB of address space.

**The incorrect answers:**

**A. 32 GB**

A 32-bit operating system does not contain 32 GB of memory addresses.

**B. 2 TB**

It's common to see 64-bit operating systems support terabytes of memory address space, but it's not available in a 32-bit operating system.

**C. 512 GB**

32-bit operating systems support a maximum of 4 GB of memory.

**D. 128 GB**

128 GB is well above the 32-bit address space of 4 GB.

**F. 16 GB**

32-bit operating systems are limited to a maximum RAM of 4 GB.



**More information:**

220-1002, Objective 1.1 - Operating Systems Overview

<https://professormesser.link/1002010101>

**C76.** A financial services company is upgrading the storage drives on their SAN and need to dispose of one hundred older storage drives. The security administrator would like to guarantee all of the drives are destroyed and the data could not be recovered. Which of the following methods would be the BEST way to accomplish this goal?

- A.** Standard format
  - B.** Full disk encryption
  - C.** Shredder
  - D.** Delete the master boot record
- 

**The Answer:** **C.** Shredder

A shredder will cut a storage drive into small pieces, and larger shredders can completely destroy a drive in just a few seconds. It would not take long to dispose of one hundred drives.

**The incorrect answers:**

**A.** Standard format

A standard format will overwrite each sector on the drive, and recovery software would not be able to undelete the data. However, the format would leave the drive functional and it would not be destroyed.

**B.** Full disk encryption

Full disk encryption would protect existing data on the drive by encrypting all of the data. This does not remove the data, and it does not destroy the drive.

**D.** Delete the master boot record

Deleting the master boot record would cause the drive to fail during boot, but none of the user data would be removed. The drive would also not be destroyed.



**More information:**

220-1002, Objective 2.9 - Data Destruction and Disposal

<https://professormesser.link/1002020901>

**C77.** A company is updating all of their UPS systems with new batteries. Which of the following would be the best way to dispose of the old batteries?

- A.** Take to a local hazardous waste facility
  - B.** Throw out with the paper trash
  - C.** Ship them to a battery wholesaler
  - D.** Bury them in a landfill
- 

**The Answer:** **A.** Take to a local hazardous waste facility

Batteries contain chemicals that are dangerous to humans and the environment. The best disposal method is to deliver the batteries to professionals at a local hazardous waste facility.

**The incorrect answers:**

**B.** Throw out with the paper trash

The batteries in a UPS are not designed to be thrown away with the normal garbage. Rechargeable batteries are fire hazards and can leak chemicals, so it's important to handle them properly.

**C.** Ship them to a battery wholesaler

A company that sells batteries does not necessarily handle the disposal of batteries. The batteries should be delivered to the local hazardous waste facility.

**D.** Bury them in a landfill

Old batteries should not be buried in a traditional landfill, and should instead be delivered to the local hazardous waste facility.



**More information:**

220-1002, Objective 4.4 - Safety Procedures

<https://professormesser.link/1002040401>

**C78.** Which of the following should a company use to reduce their legal liability if an employee is dismissed?

- A.** End user licensing agreement
  - B.** Acceptable use policy
  - C.** Knowledge base articles
  - D.** Operational procedures documentation
- 

**The Answer:** **B.** Acceptable use policy

An Acceptable Use Policy (AUP) provides detailed documentation on the acceptable use of company assets. If someone is dismissed, this document will provide a well-documented set of reasons that will help to legally justify the dismissal.

**The incorrect answers:**

**A.** End user licensing agreement

An end user licensing agreement (EULA) is a document with the terms of use for software. Most software installations include an EULA that must be accepted before the software will begin the install.

**C.** Knowledge base articles

A knowledge base article is a technical document that describes processes and procedures for completing certain tasks. A knowledge base article is generally not used or referenced during a dismissal, and it's not used to document the acceptable use of company assets.

**D.** Operational procedures documentation

Many organizations have a list of internal processes and procedures that are maintained for all systems. These operational procedures are not used as a method of documenting the acceptable use of the organization's assets.



**More information:**

220-1002, Objective 4.1 - Documentation Best Practices

<https://professormesser.link/1002040101>

**C79.** Jack, a healthcare administrator, commonly displays sensitive data on his screen as part of his normal work activities. His desk is in an open area near a busy hallway. Which of the following would add additional security to Jack's work area?

- A. Biometric door lock
  - B. Privacy filter
  - C. Cable lock
  - D. Locking cabinet
- 

**The Answer:** B. Privacy filter

A privacy filter will hide all of the information to anyone who is not sitting directly in front of the display. In an open area, this would limit the visibility of sensitive information.

**The incorrect answers:**

**A. Biometric door lock**

Jack's desk is in an open area, so there most likely wouldn't be an opportunity to use a door lock. A door lock also would not provide any additional security to the work area if the door was already open.

**C. Cable lock**

A cable lock would prevent Jack's computer from being removed from his desk, but the security that's needed is to limit the view of sensitive data. A cable lock would not provide any change to the way that information was displayed on the screen.

**D. Locking cabinet**

A locking cabinet would protect the computer system from theft, but it would not limit what information on Jack's monitor could be seen by others.



**More information:**

220-1002, Objective 2.1 - Physical Security

<https://professormesser.link/1002020101>

**C80.** Walter, a user, is trying to use a new stylus with his tablet. The screen on the tablet responds to a finger press or a swipe, but the stylus does not interact with the tablet screen. Which of the following would be the MOST likely fix for this issue?

- A. Connect to a power source
  - B. Enable Bluetooth
  - C. Upgrade to the latest OS version
  - D. Disable the Wi-Fi network
- 

**The Answer:** B. Enable Bluetooth

Most tablets use Bluetooth to connect wirelessly to external devices. If Bluetooth isn't enabled, then a stylus, wireless headphones, and other personal area network (PAN) devices will not be usable.

**The incorrect answers:**

A. Connect to a power source

The connectivity between a stylus and a tablet does not require a power source. Connecting the tablet to power will not enable or enhance the connection to the stylus.

C. Upgrade to the latest OS version

The operating system on the tablet does not commonly need to be updated to allow the use of a stylus.

D. Disable the Wi-Fi network

The Wi-Fi network connection is not related to the Bluetooth connection used by the stylus, and both the Wi-Fi and Bluetooth wireless networks can be active at the same time.



**More information:**

220-1002, Objective 3.4 - Troubleshooting Mobile Apps

<https://professormesser.link/1002030401>

**C81.** A network administrator has been asked to manage the router configurations at all company remote locations. Which of the following would be the BEST choice for this task?

- A.** SSH
  - B.** VNC
  - C.** Telnet
  - D.** RDP
- 

**The Answer:** **A.** SSH

SSH (Secure Shell) is a secure protocol that provides encrypted console communication to a remote device. SSH is commonly used to manage remote devices using their command line interfaces.

**The incorrect answers:**

**B.** VNC

VNC (Virtual Network Computing) provides screen sharing and remote control capabilities for Windows, macOS, Linux, and other operating systems. The desktop sharing capabilities of VNC are not necessary for managing router configurations at the command line.

**C.** Telnet

Telnet is an insecure terminal protocol that sends traffic across the network as non-encrypted data. Because of the lack of security related to Telnet, it is not commonly used for remote terminal communication. SSH is the secure alternative to Telnet.

**D.** RDP

RDP (Remote Desktop Protocol) allows others to view or control the screen of a Windows device. RDP would not be a common solution for configuring a router at the command line.



**More information:**

220-1002, Objective 4.9 - Remote Access Technologies

<https://professormesser.link/1002040901>

**C82.** A user is browsing to their corporate home page, but a different website appears instead. The user tries to connect with other browsers on the same computer, but the result is identical. Which of the following would be the best NEXT troubleshooting step?

- A.** Try connecting to the site in Safe Mode
  - B.** Perform an anti-malware scan
  - C.** View all browsing results in the Event Viewer
  - D.** Roll back to a previous configuration
- 

**The Answer:** **B.** Perform an anti-malware scan

If any of the browsers on a computer are being redirected to a different website, then malware would be a likely suspect. Given that all of the browsers are being redirected, there's most likely something malicious on the computer.

**The incorrect answers:**

**A.** Try connecting to the site in Safe Mode

Safe Mode would most likely not provide much difference with the method of browsing. Some services would be disabled in Safe Mode, but it's unlikely that services would have caused this issue.

**C.** View all browsing results in the Event Viewer

Event Viewer may be able to provide some additional details, but there is a lot of information to parse in the logs and it's relatively obvious that something malicious is occurring on the system. The logs will still be available afterwards if more detail is required.

**D.** Roll back to a previous configuration

There's no evidence that the current configuration is the issue. Before making any changes to the system, it would be important to determine the root cause of the issue.



**More information:**

220-1002, Objective 3.2 - Troubleshooting Security Issues  
<https://professormesser.link/1002030201>

**C83.** A technician has just received fifty boxes of used laser printer toner cartridges that were removed during an annual preventive maintenance project. Which of the following would be the best NEXT step for managing these used cartridges?

- A. Refer to the MSDS
  - B. Ship the cartridges to the original manufacturer
  - C. Dispose of the cartridges with the rest of the trash
  - D. Drill a hole in each cartridge
- 

**The Answer:** A. Refer to the MSDS

The MSDS (Material Safety Data Sheets) provide information about the safety and health associated with products in the workplace. The MSDS will document hazard information, first aid measures, handling and storage, and more.

**The incorrect answers:**

B. Ship the cartridges to the original manufacturer

The original manufacturer will most likely not be a method of disposal. There are hazardous waste and recycling centers that can properly dispose of used toner cartridges, and those would be a much better destination than the original manufacturer.

C. Dispose of the cartridges with the rest of the trash

Toner cartridges can contain residual toner and chemicals, so they should not have the same disposal process as paper and other rubbish.

D. Drill a hole in each cartridge

The toner cartridge almost certainly contains residual toner. Drilling a hole in a cartridge would not only be unnecessary, but it would most likely cause a tremendous mess. Please don't do this.



**More information:**

220-1002, Objective 4.5 - Environmental Impacts

<https://professormesser.link/1002040501>

**C84.** A system administrator has been notified that a serious security vulnerability has been identified in software used by the company. In order to quickly patch this vulnerability, the administrator has created change management documentation that will be presented to the change board. Which part of the documentation would explain the disadvantages of not quickly patching this software?

- A.** Backout plan
  - B.** End-user acceptance
  - C.** Detailed change plan
  - D.** Risk analysis
- 

**The Answer:** **D.** Risk analysis

The risk analysis provides documentation for the change board to understand the risk with making the change, and the risk if the change is not made. The board can then decide if the change is worth those risks.

**The incorrect answers:**

**A.** Backout plan

A backout plan provides a way to recover if a change did not go as planned. The backout plan does not document the disadvantages of not performing the change.

**B.** End-user acceptance

End-user acceptance is important to have before presenting to the change control board, but it does not provide any information about the risk of making (or not making) the proposed change.

**C.** Detailed change plan

The change control board will need a detailed plan that describes each step of the change. This plan will be used to make everyone aware of the scope and detail of the proposed change. The change plan does not include information about the risk associated with the proposed change.



**More information:**

220-1002, Objective 4.2 - Change Management

<https://professormesser.link/1002040201>

**C85.** A company is donating ten laptop computers to a local community center. Which of the following processes should be followed before making this donation?

- A.** Inventory management
  - B.** Acceptable use policy
  - C.** Password policy
  - D.** Knowledge base article
- 

**The Answer:** **A.** Inventory management

The donated systems must be removed from the inventory system and documentation needs to be created that will detail the donation process.

**The incorrect answers:**

**B.** Acceptable use policy

An acceptable use policy is documentation existing employees use to understand how company assets should be used.

**C.** Password policy

A password policy is created by the organization's security team to document the complexities required for passwords, the aging of password, and the password change and reset process. The password policy would not be associated with a donation of equipment.

**D.** Knowledge base article

Many organizations maintain a knowledge base of information about their internal systems and technical changes. A knowledge base is not commonly referenced when making an equipment donation.



**More information:**

220-1002, Objective 4.1 - Documentation Best Practices  
<https://professormesser.link/1002040101>

**C86.** A desktop technician would like to reinstall the Windows 10 operating system without removing any of the personal files and settings on the computer. Which of the following would be the BEST way to complete this process?

- A.** Clean installation
  - B.** Unattended installation
  - C.** Multiboot
  - D.** Refresh
- 

**The Answer:** **D.** Refresh

The Windows 10 Refresh feature provides the option for reinstalling the operating system without losing any photos, music, video, or other personal files.

**The incorrect answers:**

**A.** Clean installation

A clean installation will reinstall the Windows 10 operating system, but it will remove all of the files and settings that are currently on the system.

**B.** Unattended installation

An unattended installation will perform a normal install, but it will not prompt for user input during the process. This process can change settings and configurations, so it would not be the best choice for keeping personal files and settings.

**C.** Multiboot

A multiboot installation will install multiple operating systems onto the same computer. The user can choose which operating system to use during the startup process. Installing a second operating system as a multiboot will not use the same files and settings as the original OS.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems

<https://professormesser.link/1002010301>

**C87.** A security administrator is configuring VPN connectivity on the company smartphones and tablets. The administrator would like to ensure that the login requests are from corporate users and not unauthorized third-parties. Which of the following would provide this security feature?

- A.** Biometrics
  - B.** PIN
  - C.** Unique usernames
  - D.** Passcode
- 

**The Answer:** **A.** Biometrics

Of the available choices, the biometrics option would require the employee to be physically present when connecting to the VPN. From a smartphone or tablet, this biometric authentication would consist of a fingerprint or face recognition.

**The incorrect answers:**

**B.** PIN

A PIN (Personal Identification Number) is a number that is usually only known by the authorized individual. If a third-party gains access to the PIN, they can use it without the employee being present.

**C.** Unique usernames

Most organizations will use unique usernames for each person, rather than use a single username or share an account among multiple persons. This unique username does not ensure that the employee is physically present when authenticating.

**D.** Passcode

Like a PIN, a passcode is a secret phrase that only the employee would know. However, if a third-party gains access to the passcode, they would be able to use it without the employee being physically present.



**More information:**

220-1002, Objective 2.8 - Securing Mobile Devices  
<https://professormesser.link/1002020801>

**C88.** A company is moving three computer racks of equipment from an old data center to a new facility. Which of these safety features should be the MOST important requirement at the new location?

- A.** Air filter masks
  - B.** Anti-static mat
  - C.** Equipment grounding
  - D.** Surge protectors
- 

**The Answer:** **C.** Equipment grounding

Electrical safety is one of the most important considerations in a data center, and the equipment racks used in the data center should always be connected to an electrical ground. If an electrical fault occurs, the power will be sent to the electrical ground instead of a person.

**The incorrect answers:**

**A.** Air filter masks

Most data centers are very clean environments with very little contaminants in the air. There would not commonly be a reason to wear a filtering mask inside of a data center environment.

**B.** Anti-static mat

Anti-static mats can be useful when working inside of a computer, but they're not a significant requirement when working with equipment that's already in a computer rack.

**D.** Surge protectors

Surge protectors should certainly be part of a data center, although they're usually included with the data center's UPS (Uninterruptible Power Supply). However, the concern of electrical shock takes priority over keeping the power source as clean as possible.



**More information:**

220-1002, Objective 4.4 - Safety Procedures

<https://professormesser.link/1002040401>

**C89.** A system administrator needs to upgrade five computers at a remote site to Windows 10. Which of the following methods would perform these upgrades without requiring any input from the users?

- A.** Clean install
  - B.** Multiboot
  - C.** Unattended installation
  - D.** Repair installation
- 

**The Answer:** **C.** Unattended installation

An unattended installation will install the operating system without the need for any user intervention. The answers to the questions that would normally be presented during the installation are listed in a file, and the installation process follows those previously written instructions.

**The incorrect answers:**

**A.** Clean install

A clean install would provide a method of installing Windows, but it would require the user to provide input for all of the prompts during the installation process.

**B.** Multiboot

A multiboot installation would install two separate operating systems onto the same computer, and the user would select their choice for OS during the boot process. A multiboot installation would still require the user to answer questions during the installation process.

**D.** Repair installation

A repair installation is used to fix problems with the startup process. The repair installation will not upgrade the operating system from one version to another.



**More information:**

220-1002, Objective 1.3 - Installing Operating Systems  
<https://professormesser.link/1002010301>

**C90.** Which of the following would allow someone else in the room to maliciously obtain a username and password?

- A. Spoofing
  - B. Tailgating
  - C. DoS
  - D. Shoulder surfing
- 

**The Answer:** D. Shoulder surfing

Shoulder surfing is a low-tech method of obtaining login credentials and other sensitive information. With shoulder surfing, the attacker simply watches over the shoulder of someone else to obtain the information they need. A privacy filter can be used to minimize the chance of someone using a shoulder surfing attack.

**The incorrect answers:**

**A. Spoofing**

Spoofing is the process of impersonating another device. This is commonly accomplished by configuring a MAC (Media Access Control) address or IP (Internet Protocol) address to match an existing system on the network.

**B. Tailgating**

Tailgating is an unauthorized user gaining access to an area by using the credentials of an authorized user. Tailgating is not used to obtain usernames and passwords.

**C. DoS**

A DoS (Denial of Service) describes the process of forcing a service to fail or become unavailable. A DoS is not commonly used to obtain user credentials.



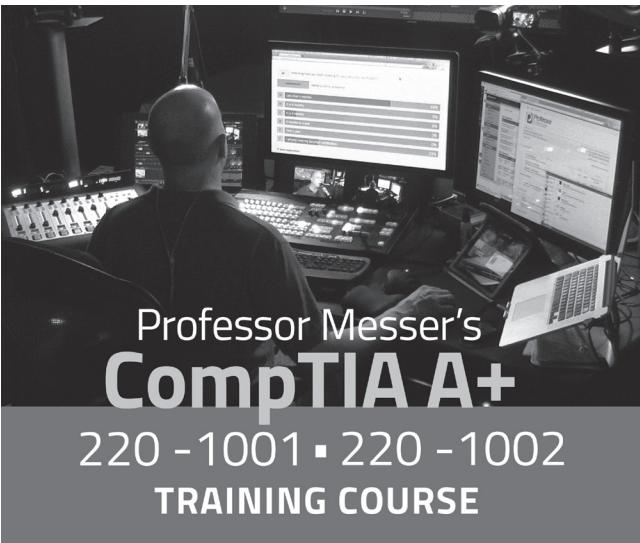
**More information:**

220-1002, Objective 2.5 - Social Engineering Attacks

<https://professormesser.link/1002020501>



Continue your journey on  
**ProfessorMesser.com:**



Professor Messer's  
**CompTIA A+**  
220-1001 • 220-1002  
**TRAINING COURSE**

**Professor Messer's CompTIA  
220-1001 and 220-1002  
A+ Training Course**

**Monthly A+ Study Group Live Streams**

**24 x 7 Live Chat**

**Professor Messer's CompTIA  
220-1001 and 220-1002  
A+ Course Notes**



# Professor Messer's **CompTIA A+**

**CORE 2** 220-1002  
**Practice Exams**

The 220-1002 Core 2 A+ Exam covers operating systems, security techniques, software troubleshooting, and more. Professor Messer's Practice Exams will familiarize students with the challenges presented by the actual Core 2 A+ exam.

#### This book includes:

- Three full-length practice exams
- Multiple-choice and performance-based questions
- Detailed explanations for each answer
- Links to additional video training for every question