

A black and white photograph showing the back of a man's head as he sits at a complex control panel, likely a video switcher or audio mixer. He is looking at several computer monitors displaying various software interfaces. One monitor shows a bar chart titled "How long have you been studying for your CompTIA security certification?" with the following data:

| Response | Percentage |
|------------------------------|------------|
| Less than 3 months | 59% |
| 3-6 months | 25% |
| 6-12 months | 10% |
| 1 year+ | 5% |
| I haven't taken the exam yet | 1% |

The man is wearing a dark t-shirt and has a lanyard around his neck. The environment is a professional studio or control room setting.

Professor Messer's **CompTIA A+**

CORE 2 220-1202
Practice Exams

James "Professor" Messer

Professor Messer's CompTIA A+ 220-1202 Core 2 Practice Exams

by James “Professor” Messer



<http://www.ProfessorMesser.com>

Professor Messer's CompTIA A+ 220-11202 Core 2 Practice Exams

Written by James "Professor" Messer

Copyright © 2025 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: May 2025

This is version 1.11

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 A+ Core 2 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 |
| Performance-Based Answers | 35 |
| Multiple Choice Detailed Answers | 43 |

Practice Exam B

| | |
|--|-----|
| Performance-Based Questions | 133 |
| Multiple Choice Questions | 139 |
| Multiple Choice Quick Answers | 165 |
| Performance-Based Answers | 167 |
| Multiple Choice Detailed Answers | 175 |

Practice Exam C

| | |
|--|-----|
| Performance-Based Questions | 263 |
| Multiple Choice Questions | 269 |
| Multiple Choice Quick Answers | 297 |
| Performance-Based Answers | 299 |
| Multiple Choice Detailed Answers | 307 |

About the Author

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

James is also the founder and CEO of Messer Studios, a leading publisher of training materials for IT certification exams. With over 235 million videos viewed and over 1.1 million subscribers, Professor Messer's training programs have helped thousands 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 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 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 CompTIA A+ 220-1202 Core 2 certification covers many different topics, and includes objectives on IT security, operating systems, and software troubleshooting. Here's the breakdown of each domain and the percentage of each topic on the A+ 220-1202 exam:

Domain 1.0 - Operating Systems- 28%

Domain 2.0 - Security - 28%

Domain 3.0 - Software Troubleshooting - 23%

Domain 4.0 - Operational Procedures- 21%

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

Performance-based questions

The first handful of questions on the A+ exam are performance-based questions. Performance-based questions are a flexible style of questioning which can take many different forms; matching, drag and drop, sorting, scenario, command-line, or nearly any other style.

Because these question types can vary, it's very difficult to accurately predict the exact style of questions which might appear on an actual exam. However, all of the performance-based questions are based on the Official CompTIA Exam Objectives, so a solid foundation in the objectives will provide the test taker with everything they need to successfully answer these questions. If you are familiar with all of the objectives, it really doesn't matter how CompTIA asks the questions.

Multiple choice questions

Unlike performance-based questions, multiple choice questions have a familiar format for most test takers. Multiple choice questions consist of a single question followed by multiple possible answers. The test taker will need to select one or more of the possible answers to successfully complete the question.

You'll need to be familiar with the style of both performance-based questions and multiple choice questions. In this book of practice exams, you'll find examples of both question types in each of the three tests.

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 A+ exams are 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 labeled "Quick Answer" or "The Details", and this link 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 which 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.

How to score the practice exams

Broadly speaking, the purpose of this book is to determine your readiness for the A+ exam. Although we've worked hard to provide you with a similar experience as the actual exam, we're not trying to reverse-engineer CompTIA's scoring system. CompTIA doesn't share the details of their scoring system, so any attempt at recreating an actual exam score would be speculative and almost certainly incorrect.

Many of the questions in this book have a single answer. If you get the question right, you would obviously give yourself one point. Some of the exam questions require multiple answers, and this is especially common with performance-based questions. With these questions, you could potentially get part of a question correct and other parts of the question incorrect.

Our recommendation is to count each question as one point, but you could also give yourself partial credit if this helps provide a better measurement of your readiness. You ultimately don't have any control over the scoring on the actual exam, so we would recommend you focus on the content and let the score provide a relative measurement of your success.

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 220-1202 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.

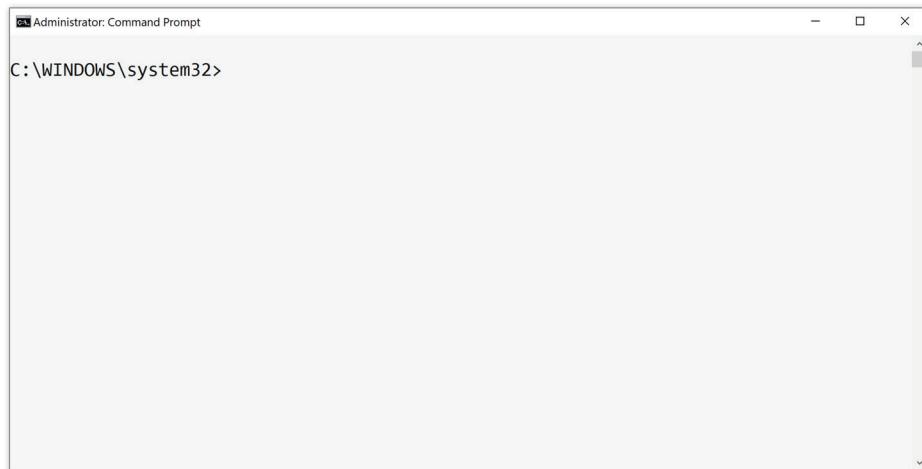
More than 81 questions correct / over 90% - You're ready for the real thing! Book your exam and pass your 220-1202 A+ exam!

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 actual exam.

Practice Exam A

Performance-Based Questions

- A1. A technician has recently removed malware from a Windows computer, but the technician is concerned 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 contains the text 'C:\WINDOWS\system32>'. The window has standard Windows-style borders and a scroll bar on the right side.

Answer Page: 35

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

- Scan and removal techniques
- Verify malware symptoms
- Remediate infected systems
- Schedule scans and run updates
- Disable System Restore
- Enable System Restore
- Educate the end user
- Reimage or reinstall
- Quarantine infected system
- Update anti-malware software

Answer Page: 36

A3. Match the best technology to the description.

Some technologies will not be matched.

PII

EULA

AUP

TOTP

GFS

FRT

BEC

A user authenticates to a mobile phone using the built-in camera

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

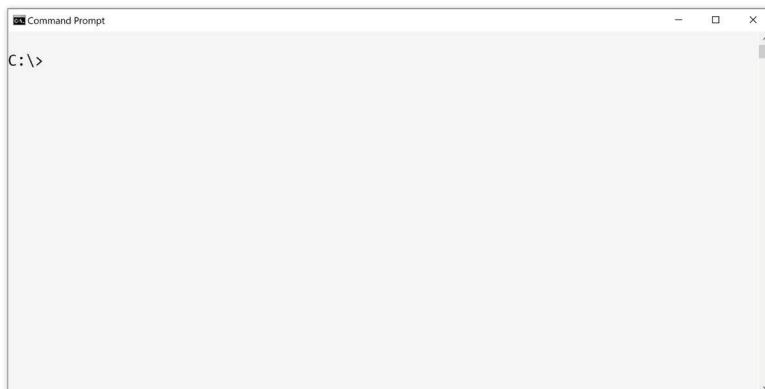
A backup series consists of monthly, weekly, and daily backup data.

The proper use of computers, tablets, and other devices is part of the employee handbook.

A user receives an email from the CEO, but the email was not actually sent by the CEO

Answer Page: 37

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:.



Answer Page: 38

- A5.** A technician has been asked to troubleshoot a problem on a Windows computer. Specify the best command to accomplish the following tasks.

Task 1: This user is a developer, and there are many different Windows computers on the user's desk. Identify the name of the Windows computer currently in use:

```
C:\Windows\system32>
```

Task 2: The client has been describing a number of connectivity issues. Check the availability of the default router located at 192.168.1.99:

```
C:\Windows\system32>
```

Task 3: To make changes to the system, the user needs to have Administrator access. Determine the logged-in username in the Windows command prompt:

```
C:\Windows\system32>
```

Task 4: The issue could be related to a problem which was solved in a recent set of updates. Identify the current OS patch level:

```
C:\Windows\system32>
```

Answer Page: 39

.....

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. Air filtration
- C. Cable management
- D. Waste disposal regulations

Quick
Answer: 33

The Details: 43

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: 216.2 GB of 512 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: 44

- A8.** A user in the accounting department is trying to install an app on their new corporate mobile phone, but the installation fails each time. Which of the following would be the most likely reason for this issue?
- A.** Incorrect file system type
 - B.** MDM policy restriction
 - C.** Slow CPU speeds
 - D.** Low battery level
- Quick
Answer: 33

The Details: 44
- A9.** A system administrator has required the use of FRT for authentication on all laptops, mobile phones, and tablets. Which of the following will be required to meet this requirement?
- A.** Fingerprint reader
 - B.** Badge reader
 - C.** Token generator
 - D.** Integrated camera
- Quick
Answer: 33

The Details: 47
- A10.** 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 the technician to include during this cleaning process?
- A.** Surge suppressor
 - B.** Temperature sensor
 - C.** Air filter mask
 - D.** ESD mat
- Quick
Answer: 33

The Details: 48
- A11.** After a user authenticates to a web site, the browser performs very slowly and some of the items on the page will not properly display. Which of the following would be the best way to resolve this issue?
- A.** Disable browser notifications
 - B.** Update the web server certificate
 - C.** Update the system BIOS
 - D.** Clear the browser cache
- Quick
Answer: 33

The Details: 49

- 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. Water hose
 - B. Foam-based extinguisher
 - C. Disconnect the power
 - D. Carbon dioxide extinguisher
- Quick
Answer: 33
The Details: 50
- A13.** Which of these Windows features provides full disk encryption for all data on a storage drive?
- A. Domain Services
 - B. EFS
 - C. RDP
 - D. BitLocker
- Quick
Answer: 33
The Details: 51
- A14.** A company maintains data retention requirements of five years for all customer names, addresses, and phone numbers. Which of the following would best describe this data?
- A. Credit card transactions
 - B. Government-issued information
 - C. PII
 - D. Healthcare data
- Quick
Answer: 33
The Details: 52
- A15.** A user in the accounting department would like to ensure their mobile device data is always available. If the user's smartphone is damaged or stolen, they would like to replace the device and restore all data as quickly as possible. Which of the following would provide this functionality?
- A. Full device encryption
 - B. Remote backup
 - C. IoT isolation
 - D. Remote wipe
- Quick
Answer: 33
The Details: 53

- A16.** Each time a user starts a specific corporate application, a page of disclaimers and usage requirements is shown before the login prompt. Which of the following would best describe this page?
- A. Splash screen
 - B. Acceptable use policy
 - C. Standard operating procedures
 - D. Topology diagram
- A17.** A system administrator is troubleshooting an older application on a Windows 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
- 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 the building has an electrical ground
 - C. Connect a surge suppressor to each system
 - D. Maintain an inventory of replacement power supplies
- 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: 54

Quick
Answer: 33

The Details: 55

Quick
Answer: 33

The Details: 56

Quick
Answer: 33

The Details: 57

A20. 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: 58

A21. An attacker is using every combination of letters, numbers, and special characters in an attempt to discover a user's password. Which of the following would describe this attack type?

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

Quick
Answer: 33

The Details: 59

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

Quick
Answer: 33

The Details: 60

- A23.** When connecting a new USB webcam to Windows 11, a message appears stating "The controller does not have enough resources for this device." Which of the following would be the best next troubleshooting step?
- A. Close all large-memory processes
 - B. Modify the BCD
 - C. Move the webcam to a different USB interface
 - D. Use System Restore to rollback to a previous configuration
- A24.** A system administrator has created a shared folder on a server to store operating system images. Technicians 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
- A25.** A system administrator is installing a Windows Server device in the data center. Which of the following file systems would be the best choice for this task?
- A. ReFS
 - B. APFS
 - C. ext4
 - D. XFS

Quick
Answer: 33

The Details: 61

Quick
Answer: 33

The Details: 62

Quick
Answer: 33

The Details: 63

A26. A security technician has identified malware running in 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.** Cryptominer

Quick
Answer: **33**

The Details: **64**

A27. A help desk technician has been called to a training room with Android tablets as presentation devices. An application used during 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

Quick
Answer: **33**

The Details: **65**

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 appeared 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

Quick
Answer: **33**

The Details: **66**

- 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 a person 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
- A31.** A Linux administrator needs to modify the configuration text file for a service. Which of the following utilities would provide this functionality?
- A.** nano
 - B.** chmod
 - C.** df
 - D.** sudo
- A32.** An internal audit has found a server in the DMZ which appears to be infected with malware. The malware does not appear to be part of a file in the OS, and the malware runs each time the system is started. What type of malware would be most likely found on this server?
- A.** Trojan
 - B.** Ransomware
 - C.** Keylogger
 - D.** Spyware
 - E.** Boot sector virus

Quick
Answer: 33

The Details: 67

Quick
Answer: 33

The Details: 68

Quick
Answer: 33

The Details: 69

Quick
Answer: 33

The Details: 70

A33. A user has delivered a broken laptop to the help desk, and they are visibly upset and quite vocal about the problem they're having. The user is also asking for a very specific repair which 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: 71

A34. 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, the phone is displaying a large number of advertisements when browsing the Internet. Which of the following tasks should the user perform after completing a factory reset?

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

Quick
Answer: 33

The Details: 72

A35. When making configuration changes, a technician is assigned a temporary administrator password to use for the duration of the update. Once the administrator credentials are used, they are automatically deleted. Which of the following would best describe this process?

- A.** Single sign-on
- B.** Data loss prevention
- C.** User Access Console
- D.** Just-in-time access

Quick
Answer: 33

The Details: 73

- A36.** A user has been provided with a username and password for accessing the corporate VPN. The user has also been provided with a hardware device displaying a six digit code, and the code changes every 30 seconds. Which of the following would best describe the use of this device?
- A.** ACL
 - B.** Group Policy
 - C.** SMS
 - D.** Least privilege
 - E.** MFA
- 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.** Performance Monitor
 - C.** Task Manager
 - D.** robocopy
- 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

Quick
Answer: 33

The Details: 75

Quick
Answer: 33

The Details: 76

- 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 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
 - C. Regular format
 - D. Reinstall the operating system
- Quick
Answer: 33
The Details: 77
- 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 folder the current directory?
- A. cd logs
 - B. mv logs
 - C. dir logs
 - D. md logs
- Quick
Answer: 33
The Details: 78
- A41.** A system administrator is configuring a server to use eight bootable partitions on a single SSD. Which of the following partition styles would be the best choice for this configuration?
- A. MBR
 - B. NTFS
 - C. diskpart
 - D. GPT
- Quick
Answer: 33
The Details: 79

- A42.** A technician is installing a fresh Windows operating system on a file server. Unfortunately, the drive controller in the system is not recognized during the installation process. Which of the following would be the best way to manage this issue?
- A.** Load third-party drivers
 - B.** Restart the system
 - C.** Use a remote network installation
 - D.** Boot from the recovery partition
- Quick
Answer: 33
- A43.** A security administrator is concerned a bad actor may use packet analysis to determine a list of web sites visited by their users. Which of the following would prevent this type of reconnaissance?
- A.** Enable full disk encryption
 - B.** Login with multifactor authentication
 - C.** Use a secure DNS
 - D.** Configure the BIOS for Secure Boot
- The Details: 80
- A44.** A user in the sales department is attempting to upgrade the operating system of their smartphone, but the smartphone will not start the installation when selected. Which of the following is the most likely reason for this issue?
- A.** Bluetooth is enabled
 - B.** The smartphone storage is nearly full
 - C.** Rotation lock is disabled
 - D.** The phone is connected to a power source
- Quick
Answer: 33
- The Details: 82

- A45.** The hard drive in a macOS desktop has failed and none of the data on the drive is 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. Mission Control
 - 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 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 an open-source license
 - C. The user has installed a personal license
 - D. The software requires a USB key for DRM
- A47.** A system administrator is upgrading four workstations from Windows 8.1 to Windows 11. 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. In-place upgrade
- 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: 83

Quick
Answer: 33

The Details: 84

Quick
Answer: 33

The Details: 85

Quick
Answer: 33

The Details: 86

- A49.** A technician has been called to resolve an issue with a networked laser printer 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.** A system administrator is starting a Windows computer, but during startup they receive the message, "One or more services failed to start." Additional reboots result in the same error message. Which of the following would be the best next troubleshooting step?
- A.** Check for proper cooling
 - B.** Run a hardware diagnostic
 - C.** Modify the service permissions
 - D.** Rebuild the BCD
- A51.** A system administrator would like all help desk computers to check for anti-virus signature updates every hour during the workday. Which of the following would be the best way to provide this functionality?
- A.** System Configuration
 - B.** Task Scheduler
 - C.** Device Manager
 - D.** Certificate Manager
 - E.** SFC

Quick
Answer: 33

The Details: 87

Quick
Answer: 33

The Details: 88

Quick
Answer: 33

The Details: 89

- A52.** A workstation on a manufacturing floor is taking much longer to boot than normal. 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
- A53.** A Windows user is installing a new application, and the installation process 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 Details: 91
- 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.** WPA3 settings
 - B.** Outdated anti-virus signatures
 - C.** Disconnected VPN
 - D.** MDM configuration
- Quick
Answer: 33
- The Details: 92
- A55.** An employee has modified the NTFS permissions on a folder 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: 93

- 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 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
- A57.** A technician was assigned a support ticket with an urgently requested a laptop screen repair. The support team was able to locate a replacement and install a new LCD display in less than 24 hours. The laptop was returned to the user and the user immediately left on a business trip. Which of the following would be the best next step for this repair?
- A. Order a backup replacement display
 - B. Update the user's login script
 - C. Run diagnostics on the original screen
 - D. Contact the user to verify satisfaction
- A58.** A user has received a pop up message on their computer stating applications on their computer are infected with a virus. A technician has determined the pop up message is a hoax and it 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 the original installation media

Quick
Answer: 33

The Details: 94

Quick
Answer: 33

The Details: 95

Quick
Answer: 33

The Details: 96

A59. A network administrator needs to manage a switch and a firewall in the local data center. Which of the following would be the best choice for this requirement?

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

Quick
Answer: 33

The Details: 97

A60. A user is using a smartphone at their desk, and they occasionally receive a security warning in the browser. After some additional troubleshooting, the technician determines the security warnings are fake. 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: 98

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

- A.** Create a login script
- B.** Install the latest OS patches
- C.** Run SFC
- D.** Modify the BIOS boot order

Quick
Answer: 33

The Details: 99

- A62.** A user has opened a help desk ticket relating to desktop alerts randomly appearing throughout the day. Most of the alerts contain information about third-party products and services. Which of the following is the most likely cause of these messages?
- A. On-path attack
 - B. Corrupted email database
 - C. OS update failure
 - D. Adware
- 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
- 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. winver
 - C. sfc
 - D. diskpart

A65. A desktop administrator has determined 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 which 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: 103

A66. A system administrator would like to require a specific level of 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: 104

A67. A system administrator is creating a series of shared folders which should not be visible when users browse the network for available 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: 105

- A68.** 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. The user has confirmed 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 disabled
 - 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 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 which 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

Quick
Answer: 33

The Details: 106

Quick
Answer: 33

The Details: 107

Quick
Answer: 33

The Details: 108

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: 109

A72. A financial management company would like to ensure 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. UPnP
- C. Multi-factor authentication
- D. TKIP
- E. TACACS
- F. Kerberos
- G. WPA3

Quick
Answer: 33

The Details: 110

A73. A network consulting firm is upgrading the Internet firewalls for a large corporation. The proposal includes a description of the project and the network topology changes required to support the upgrade. The proposal also describes the risks involved with making this upgrade. Which of the following would be the last step in this upgrade?

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

Quick
Answer: 33

The Details: 112

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: 113

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 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: 114

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: 115

A77. A financial corporation is deploying laptops to their salespeople in the field. The sales teams require video playback functionality, but the Windows configuration does not include any multimedia utilities. Which of the following would be the most likely reason for these missing utilities?

- A.** Laptops are using Windows N edition
- B.** Video playback is disabled in the BIOS
- C.** Laptop hardware does not support video playback
- D.** The video format is not recognized by the laptop

Quick
Answer: 33

The Details: 116

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: 117

A79. While using a Windows laptop during presentations, a company vice president has reported her system is interrupting the meeting with system notifications from the browser, PDF reader, the Microsoft Store, and other applications. Which of the following would be the best way to address this issue?

- A.** Use a different laptop for presentations
- B.** Run the presentation software as Administrator
- C.** Enable Airplane mode while presenting
- D.** Disable notifications while specific applications are running

Quick
Answer: 33

The Details: 118

- A80.** A system administrator needs to upgrade a training room of twenty systems to the latest Windows version. Which of the following would be the most efficient method of performing this upgrade process?
- A. Recovery partition
 - B. Remote network installation
 - C. Repair installation
 - D. USB key
- Quick
Answer: 33
- 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 the computer, 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 Details: 119
- A82.** An employee at a company is responsible for determining the correct access controls for each user, manage the authentication process, and track all access to network resources. Which of the following would best describe this employee's job function?
- A. PAM
 - B. DLP
 - C. MDM
 - D. IAM
- Quick
Answer: 33
- The Details: 120

A83. 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. While testing other website connections on the computer, the technician finds 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: 122

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.** Restrict log-in times for the partner account
- 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: 123

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
- C.** dig
- D.** sudo

Quick
Answer: 33

The Details: 124

A86. A user is connecting their laptop to an external monitor and keyboard, but the laptop goes into sleep mode if the laptop screen is shut. Which of the following utilities can be used to keep the laptop running when the lid is closed?

- A.** Power Options
- B.** Device Manager
- C.** Personalization
- D.** User Accounts

Quick
Answer: 33

The Details: 125

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.** Secure management access
- D.** DHCP reservation
- E.** IP filtering

Quick
Answer: 33

The Details: 126

A88. A company maintains a Windows system in the conference room for use during meetings. However, the system has not received any recent updates and will no longer connect to the corporate network due to missing security patches. Which of the following would be the most likely reason for this issue?

- A.** BIOS administrator password is enabled
- B.** No users are actively logged in
- C.** Firewall is filtering traffic
- D.** Guest accounts are disabled

Quick
Answer: 33

The Details: 128

A89. A company is deploying laptops to all of their field sales teams. The company is concerned about protecting the security of data if the laptop is stolen or misplaced. Which of the following would be the best way to address this concern?

- A.** Multifactor authentication
- B.** Strong password policies
- C.** Unique device certificates
- D.** Data-at-rest encryption

Quick
Answer: 33

The Details: 129

A90. A company has discovered a recent data breach, and this breach appears to have originated through a vulnerability introduced with a software upgrade. The vulnerability was added by the attacker at the source and distributed to all customers who performed the upgrade. Which of the following would best describe this attack type?

- A.** Supply chain attack
- B.** Insider threat
- C.** Business email compromise
- D.** On-path attack

Quick
Answer: 33

The Details: 130

Practice Exam A

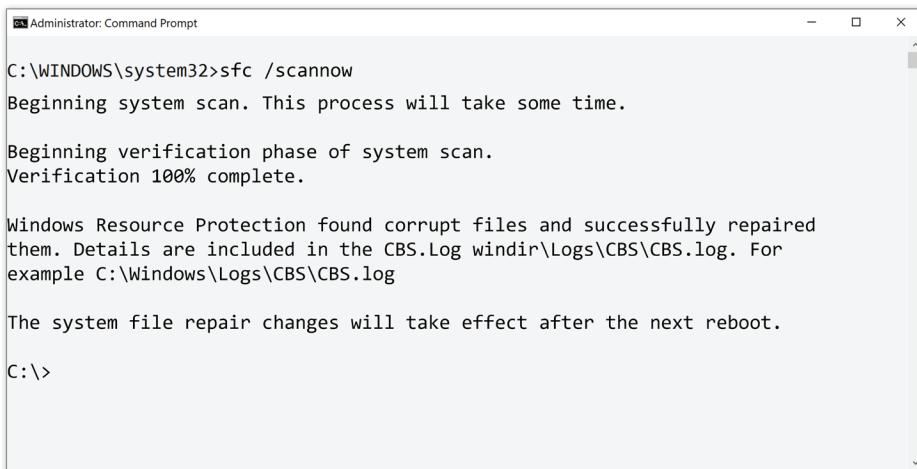
Multiple Choice Quick Answers

- | | | |
|--------|--------|--------------|
| 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

Performance-Based Answers

- A1. A technician has recently removed malware from a Windows computer, but the technician is concerned 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 which may be corrupted.



More information:

220-1202, Objective 1.5 - Windows Command Line Tools
<https://professormesser.link/1202010501>

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

Verify malware symptoms

Quarantine infected system

Disable System Restore

Remediate infected systems

Update anti-malware software

Scan and removal techniques

Reimage or reinstall

Schedule scans and run updates

Enable System Restore

Educate the end user

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:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

A3. Match the best technology to the description.

Some technologies will not be matched.

FRT

A user authenticates to a mobile phone using the built-in camera

FRT (Facial Recognition Technology) is often used as an authentication factor and uses a built-in camera to scan and verify a user's facial features.

PII

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

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

GFS

A backup series consists of monthly, weekly, and daily backup data.

GFS (Grandfather, Father, Son) is a backup strategy using three different backup intervals to maintain and manage large amounts of data. The grandfather backup is generally done once a month, the father backups are performed weekly, and the son backups are captured each day.

AUP

The proper use of computers, tablets, and other devices is part of the employee handbook.

An AUP (Acceptable Use Policy) is a set of rules, regulations, or policies used to document the proper use of technology devices and software. These guidelines are often managed through the employee handbook.

BEC

A user receives an email from the CEO, but the email was not actually sent by the CEO

BEC (Business Email Compromise) is often used by an attacker to send fraudulent email messages to a victim.

Not used:

EULA - End User Licensing Agreement - Determines how the software can be used by the end user.

TOTP - Time-based One-time Password - Some authentication methods require an additional factor, and this is often a code provided by a TOTP app.

- 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:

220-1202, Objective 1.5

The Windows Network Command Line

<https://professormesser.link/1202010502>

- A5.** A technician has been asked to troubleshoot a problem on a Windows computer. Specify the best command to accomplish the following tasks.

Task 1: This user is a developer, and there are many different Windows computers on the user's desk. Identify the name of the Windows computer currently in use:

```
C:\Windows\system32> hostname  
Laptop42
```

The hostname command simply displays the name of the host at the command line. This can be a very useful utility when many remote console windows are open or the name of the system is not known. In this example, the name of the Windows device is "Laptop42."

Task 2: The client has been describing a number of connectivity issues. Check the availability of the default router located at 192.168.1.99:

```
C:\Windows\system32> ping 192.168.1.99  
  
Pinging 192.168.1.99 with 32 bytes of data:  
Reply from 192.168.1.99: bytes=32 time=9ms TTL=64  
Reply from 192.168.1.99: bytes=32 time=9ms TTL=64  
Reply from 192.168.1.99: bytes=32 time=10ms TTL=64  
Reply from 192.168.1.99: bytes=32 time=5ms TTL=64  
  
Ping statistics for 192.168.1.99:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 5ms, Maximum = 10ms, Average = 8ms
```

The ping command is used to check the availability of a device and to calculate round-trip times. The router at 192.168.1.99 has responded to all four requests and round trip times are averaging 8 milliseconds.

Task 3: To make changes to the system, the user needs to have Administrator access. Determine the logged-in username in the Windows command prompt:

```
C:\Windows\system32> whoami  
company1\professor
```

Identifying the current logged-in user can be important when troubleshooting. On this computer, the logged in user is on the Active Directory domain named "company1," and the current user is "professor."

Task 4: The issue could be related to a problem which was solved in a recent set of updates. Identify the current OS patch level:

```
C:\Windows\system32> winver
```

The winver (Windows Version) command launches the "About Windows" dialog box from the command prompt:



More information:

220-1202, Objective 1.5 - Windows Command Line Tools
<https://professormesser.link/1202010501>



More information:

220-1202, Objective 1.5 -
The Windows Network Command Line
<https://professormesser.link/1202010502>

Practice Exam A

Multiple Choice Detailed Answers

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.** Air filtration
 - 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. Air filtration

Cleaning the inside of a system or printer can cause dust and particles to become airborne. Using a mask or air filtration system can keep those particles out of your mouth, nose, and lungs.

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:

220-1202, Objective 4.4 - Safety Procedures

<https://professormesser.link/1202040402>

- 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: 216.2 GB of 512 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 which 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 which 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:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

- A8.** A user in the accounting department is trying to install an app on their new corporate mobile phone, but the installation fails each time. Which of the following would be the most likely reason for this issue?
- A.** Incorrect file system type
 - B.** MDM policy restriction
 - C.** Slow CPU speeds
 - D.** Low battery level
-

The Answer: **B.** MDM policy restriction

An MDM (Mobile Device Manager) provides centralized management and administration for all mobile phones, tables, and other mobile devices. In this example, the MDM is most likely restricting the installation of any unauthorized apps.

The incorrect answers:

A. Incorrect file system type

The file systems used on mobile devices are not commonly configurable by the end user, and it's unlikely a different file system would have been installed on the mobile phone.

C. Slow CPU speeds

CPU (Central Processing Unit) speeds can be important for high-performance computing requirements, but a mobile device can generally complete an app installation with any installed processor.

D. Low battery level

We rely on a good battery level to ensure the best possible performance from our mobile phones, but a low battery would not generally prevent the installation of a new application.



More information:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

- A9.** A system administrator has required the use of FRT for authentication on all laptops, mobile phones, and tablets. Which of the following will be required to meet this requirement?
- A.** Fingerprint reader
 - B.** Badge reader
 - C.** Token generator
 - D.** Integrated camera
-

The Answer: **D.** Integrated camera

FRT (Facial Recognition Technology) is a common authentication method and requires the use of a camera or imaging system. Laptops, mobile phones, and tablets often integrate a camera into the hardware of the device.

The incorrect answers:

A. Fingerprint reader

A fingerprint reader is often integrated into laptops keyboards and it makes it convenient to use a biometric factor during authentication. However, a fingerprint reader is not commonly used for facial recognition.

B. Badge reader

A badge reader can be used to authenticate to a device or unlock a door, but it's not a common authentication factor for mobile phones or tablets.

C. Token generator

A USB token is often used as a separate authentication factor, but a token generator is not a replacement for facial recognition.



More information:

220-1202, Objective 2.1 - Physical Access Security

<https://professormesser.link/1202020102>

A10. 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 the technician to include during this cleaning process?

- A. Surge suppressor
 - B. Temperature sensor
 - C. Air filter mask
 - D. ESD mat
-

The Answer: C. Air filter mask

A technician working with dust or debris in the air should use an air filter mask to prevent any particles in the air from entering their lungs.

The incorrect answers:

A. Surge suppressor

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

B. Temperature sensor

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

D. ESD mat

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



More information:

220-1202, Objective 4.4 - Safety Procedures
<https://professormesser.link/1202040402>

A11. After a user authenticates to a web site, the browser performs very slowly and some of the items on the page will not properly display. Which of the following would be the best way to resolve this issue?

- A.** Disable browser notifications
 - B.** Update the web server certificate
 - C.** Update the system BIOS
 - D.** Clear the browser cache
-

The Answer: **D.** Clear the browser cache

The browser cache contains a copy of information downloaded on previous visits to a website. If this local cache is not updated with newer web page information, the website performance may be degraded. Clearing the cache can resolve this conflict and allow the browser to store a new copy of the web page.

The incorrect answers:

A. Disable browser notifications

Browser notifications can be informational, but they would not commonly cause a website to perform slowly or show an incomplete page.

B. Update the web server certificate

An invalid web server certificate will cause issues with the encryption and trust associated with a site, but it would not commonly be associated with poor performance or slowdowns.

C. Update the system BIOS

It's important to keep the BIOS updated for security and performance reasons, but the BIOS is not commonly associated with performance issues in a browser.



More information:

220-1202, Objective 3.4 - Troubleshooting Security Issues

<https://professormesser.link/1202030401>

- 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. Water hose
 - B. Foam-based extinguisher
 - C. Disconnect the power
 - D. Carbon dioxide extinguisher
-

The Answer: D. 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. Water hose

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

B. 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:

220-1202, Objective 4.4 - Safety Procedures

<https://professormesser.link/1202040402>

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

- A.** Domain Services
 - B.** EFS
 - C.** RDP
 - 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 NTFS (NT File System) to provide encryption at the file system level. Individual files and folders can be encrypted in Windows using EFS.

C. RDP

RDP (Remote Desktop Protocol) is commonly used to remotely control the desktop of a Windows computer. RDP is not used for encryption of files on the system.



More information:

220-1202, Objective 1.3 - Windows Features

<https://professormesser.link/1202010302>

A14. A company maintains data retention requirements of five years for all customer names, addresses, and phone numbers. Which of the following would best describe this data?

- A.** Credit card transactions
 - B.** Government-issued information
 - C.** PII
 - D.** Healthcare data
-

The Answer: C. PII

PII (Personally Identifiable Information) is any data which could be used to identify an individual. A name, address, and phone number would be common examples of PII.

The incorrect answers:

A. Credit card transactions

Financial information is considered to be sensitive information, and the credit card number and transaction details are important data security concerns.

B. Government-issued information

Governments commonly issue documents and identification cards to support government services for their citizens. A person's name, address, and phone number are not commonly issued by a governmental entity.

D. Healthcare data

Healthcare data often contains health status information, health care records, and more. A persons name, address, and phone number are not considered to be related to healthcare data.



More information:

220-1202, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1202040602>

A15. A user in the accounting department would like to ensure their mobile device data is always available. If the user's smartphone is damaged or stolen, they would like to replace the device and restore all data as quickly as possible. Which of the following would provide this functionality?

- A.** Full device encryption
 - B.** Remote backup
 - C.** IoT isolation
 - D.** Remote wipe
-

The Answer: **B.** Remote backup

A cloud-based remote backup solution will constantly backup all user data to a remote service. If the device is replaced, all of the user data can be restored directly from this backup in the cloud.

The incorrect answers:

A. Full device encryption

Most remote devices support encryption of all data stored on the system. With this encryption enabled, a third-party with physical access to the mobile device would not be able to access the data.

C. IoT isolation

IoT (Internet of Things) devices can provide smart machines and wearable devices, but isolating IoT devices to their own network would not provide data recovery if a system was no longer available.

D. Remote wipe

If a device is stolen, it's useful to send a remote wipe command to delete everything on the device. This functionality would not backup or restore the user's data, however.



More information:

220-1202, Objective 2.8 - Mobile Device Security

<https://professormesser.link/1202020801>

A16. Each time a user starts a specific corporate application, a page of disclaimers and usage requirements is shown before the login prompt. Which of the following would best describe this page?

- A.** Splash screen
 - B.** Acceptable use policy
 - C.** Standard operating procedures
 - D.** Topology diagram
-

The Answer: **A.** Splash screen

A splash screen displays a message, logo, or graphic during the startup process. This screen often contains a legal disclaimer regarding access to the system and information about the data contained in the application.

The incorrect answers:

B. Acceptable use policy

An acceptable use policy (AUP) is a formal set of rules and regulations, and it's usually maintained in a central repository such as the employee handbook.

C. Standard operating procedures

Standard operating procedures (SOP) are a set of procedures for handling operations, software upgrades, and other normal and expected business functions. A list of standard operating procedures would not be shown when an application is started.

D. Topology diagram

Topology diagrams are useful for identifying the configuration of switches, routers, and other infrastructure devices. A topology diagram is not shown during the startup process for an application.



More information:

220-1202, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1202040602>

A17. A system administrator is troubleshooting an older application on a Windows 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:



220-1202, Objective 2.2 - Windows Security Settings



<https://professormesser.link/1202020203>

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 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 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:

220-1202, Objective 4.5 - Environmental Impacts

<https://professormesser.link/1202040501>

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 is limited to 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:

220-1202, Objective 1.10 - Installing Applications

<https://professormesser.link/1202011001>

A20. 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 list 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 which 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:

220-1202, Objective 1.4



The Microsoft Management Console

<https://professormesser.link/1202010402>

A21. An attacker is using every combination of letters, numbers, and special characters in an attempt to discover a user's password. Which of the following would describe this attack type?

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

The Answer: C. Brute force attack

A brute force attack works to determine a user's password by trying every possible combination of letters, numbers, and special characters until the proper combination is found.

The incorrect answers:

A. Spoofing

Spoofing is a technique where one device pretends to be another device. Trying every possible password option would not be associated with a spoofing attack.

B. Social engineering

Social engineering is an attack method using many different psychological techniques to obtain access or information. A brute force attack is not categorized as social engineering.

D. DDoS

DDoS (Distributed Denial of Service) is an attack type using many different and distributed systems to force a service to fail. A brute force attack is not associated with a DDoS attack.



More information:

220-1202, Objective 2.5 - Password Attacks

<https://professormesser.link/1202020505>

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

The Answer: **A.** Rollback plan

Even with the best planning, there can always be unexpected events. Every proposed change needs to have a rollback plan in case the environment needs to be returned to its original state.

The incorrect answers:

B. Disaster recovery plan

A disaster recovery plan applies to major events which impact a large portion of an organization. A failed email upgrade does not meet the scope of 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:

220-1202, Objective 4.2 - Change Management

<https://professormesser.link/1202040201>

A23. When connecting a new USB webcam to Windows, a message appears stating "The controller does not have enough resources for this device." Which of the following would be the best next troubleshooting step?

- A. Close all large-memory processes
 - B. Modify the BCD
 - C. Move the webcam to a different USB interface
 - D. Use System Restore to rollback to a previous configuration
-

The Answer: C. Move the webcam to a different USB interface

The resources associated with a USB (Universal Serial Bus) interface can vary based on the interface type and USB controller version. If these resources are exceeded on a USB controller, the system will display a message regarding the lack of resources.

The incorrect answers:

A. Close all large-memory processes

The resources associated with the USB interface are not related to the available RAM in the operating system.

B. Modify the BCD

The Windows BCD (Boot Configuration Data) is used during startup to identify the location of the Windows installation. Updating the BCD will not resolve USB-related resource contention.

D. Use System Restore to rollback to a previous configuration

This issue is related to the hardware connected to a USB controller. Changing the configuration of the operating system will not resolve this issue.



More information:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

A24. A system administrator has created a shared folder on a server to store operating system images. Technicians 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 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:

220-1202, Objective 1.7 - Windows Network Technologies

<https://professormesser.link/1202010701>

A25. A system administrator is installing a Windows Server device in the data center. Which of the following file systems would be the best choice for this task?

- A.** ReFS
 - B.** APFS
 - C.** ext4
 - D.** XFS
-

The Answer: **A.** ReFS

ReFS (Resilient File System) is a Windows file system supporting large storage systems and a focus on data availability.

The incorrect answers:

B. APFS

APFS (Apple File System) is a file system commonly found on Apple operating systems such as macOS, iOS, and iPadOS.

C. ext4

The ext4 (Fourth Extended File System) is common to Linux, the Android operating system, and other similar OSes.

D. XFS

XFS (Extended File System) is a high performance file system for Linux. XFS would not commonly be associated with a Windows Server installation or configuration.



More information:

220-1202, Objective 1.1 - File Systems

<https://professormesser.link/1202010102>

A26. A security technician has identified malware running in 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.** Cryptominer
-

The Answer: **A.** Rootkit

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

The incorrect answers:

B. Worm

A virus needs a user to click on a file or execute an application. A worm doesn't need any human intervention and can self-replicate between systems without any additional clicks.

C. Botnet

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

D. Cryptominer

A cryptominer is malware used to perform mathematical calculations in an effort to accumulate a cryptocurrency. This malware often uses extensive CPU cycles and causes performance issues on the system.



More information:

220-1202, Objective 2.4 - Malware

<https://professormesser.link/1202020401>

A27. A help desk technician has been called to a training room with Android tablets as presentation devices. An application used during 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 significant changes would be required.

The incorrect answers:

A. Install all operating system updates

Making a change to the system without understanding the issue could cause additional problems. 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:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

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 appeared 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 from a completely different operating system or to no operating system at all. This would not commonly 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:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

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 64-bit operating systems, 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 a significant difference when installing an application on a 32-bit operating system compared to 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 the installation process.



More information:

220-1202, Objective 1.10 - Installing Applications

<https://professormesser.link/1202011001>

A30. A security guard has reported a person 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 who 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 which rotates through 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:

220-1202, Objective 2.5 - Social Engineering

<https://professormesser.link/1202020501>

A31. A Linux administrator needs to modify the configuration text file for a service. Which of the following utilities would provide this functionality?

- A.** nano
 - B.** chmod
 - C.** df
 - D.** sudo
-

The Answer: **A.** nano

The nano utility is a full-screen text editor available from the command line of a Linux device.

The incorrect answers:

B. chmod

The chmod (Change Mode) utility is used to modify the read, write, or execution permissions of an object in the Linux file system.

C. df

The df (Disk Free) utility provides a view of available filesystems and the free disk space in each filesystem.

D. 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 text editing functionality.



More information:



220-1202, Objective 1.9 - Linux Commands Part 2



<https://professormesser.link/1202010902>

A32. An internal audit has found a server in the DMZ which appears to be infected with malware. The malware does not appear to be part of a file in the OS, and the malware runs each time the system is started. What type of malware would be most likely found on this server?

- A.** Trojan
 - B.** Ransomware
 - C.** Keylogger
 - D.** Spyware
 - E.** Boot sector virus
-

The Answer: **E.** Boot sector virus

Some boot sectors can be modified to run malware, and this means the malicious software is started each time the computer is booted. The Secure Boot features in a modern UEFI BIOS can prevent unsigned malicious software from running during the startup process.

The incorrect answers:

A. Trojan

A Trojan horse is malware pretending to be legitimate software. In this example, there was no mention of any specific software running in the operating system.

B. Ransomware

Ransomware is malware which encrypts all of your personal files. Ransomware often requires a payment, or ransom, to regain access to the data.

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 used to monitor browsing locations, capture keystrokes, and watch user activity.



More information:

220-1202, Objective 2.4 - Malware

<https://professormesser.link/1202020401>

A33. A user has delivered a broken laptop to the help desk, and they are visibly upset and quite vocal about the problem they're having. The user is also asking for a very specific repair which 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 which would be associated with emotion. Technical problems can be stressful enough on their own, and adding to the conflict 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 an open line of communication.



More information:

220-1202, Objective 4.7 - Communication

<https://professormesser.link/1202040702>

A34. 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, the phone is displaying a large number of advertisements when browsing the Internet. Which of the following tasks should the user perform after completing a factory reset?

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

The Answer: **D.** Verify the source of each app before installation
It's always a good best practice to check the legitimacy of each app installed on a smartphone. In this example, it's likely one of the apps is infected with malware.

The incorrect answers:

A. Disable Bluetooth

Given the limited information in the question, there's no evidence Bluetooth was related to the advertising 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 a system to display advertisements.

C. Run a speed test on the cellular connection

The speed of a cellular network connection would not cause a smartphone to display unwanted and excessive advertisements.



More information:

220-1202, Objective 3.3 -

Troubleshooting Mobile Device Security

<https://professormesser.link/1202030301>

A35. When making configuration changes, a technician is assigned a temporary administrator password to use for the duration of the update. Once the administrator credentials are used, they are automatically deleted. Which of the following would best describe this process?

- A. Single sign-on
 - B. Data loss prevention
 - C. User Access Control
 - D. Just-in-time access
-

The Answer: D. Just-in-time access

Just-in-time access describes the temporary assignment of authentication credentials or permissions. Credentials are created temporarily and deleted once the session is complete. This process prevents any ongoing misuse of the credentials by a bad actor.

The incorrect answers:

A. Single sign-on

The single sign-on process prompts for authentication credentials once, and then uses those credentials for a period of time without requiring any additional user input.

B. Data loss prevention

Data loss prevention focuses on preventing the unintentional (or intentional) disclosure of sensitive information. Data loss prevention solutions can identify and block this sensitive information sent using an application or across the network.

C. User Access Control

User Access Control (UAC) is a Windows feature designed to prevent unauthorized changes to the Windows operating system. UAC is not used as a temporary administrator authentication method.



More information:

220-1202, Objective 2.1 - Authentication and Access

<https://professormesser.link/1202020104>

A36. A user has been provided with a username and password for accessing the corporate VPN. The user has also been provided with a hardware device displaying a six digit code, and the code changes every 30 seconds. Which of the following would best describe the use of this device?

- A.** ACL
 - B.** Group Policy
 - C.** SMS
 - D.** Least privilege
 - E.** MFA
-

The Answer: E. MFA

MFA (Multi-factor Authentication) adds an additional security factor to the authentication process. Instead of using only a username and password (something you know), additional factors are required to login. In this example, the hardware device creates a pseudo-random code to be included with the login process.

The incorrect answers:

A. ACL

An ACL (Access Control List) allows or denies access to a resource. The device in this question would not provide any control of a resource.

B. Group Policy

Windows Domains can use Group Policy to define and manage configurations of end-user devices.

C. SMS

SMS (Short Message Service) is a text message. Although it's a common form of MFA, text messaging is not used in this example.

D. Least privilege

The principle of least privilege ensures users only have the rights and permissions necessary to perform their minimum job function.



More information:

220-1202, Objective 2.1 - Logical Security

<https://professormesser.link/1202020103>

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.** Performance Monitor
 - C.** Task Manager
 - D.** robocopy
-

The Answer: **C.** Task Manager

The Windows Task Manager includes a Startup tab for managing the applications which launch during the login 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. Performance Monitor

The Performance Monitor utility is designed to collect metrics over an extended period of time. Performance Monitor does not provide any management or control of the startup process.

D. robocopy

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



More information:

220-1202, Objective 1.4 - Task Manager

<https://professormesser.link/1202010401>

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 any 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 (Electrostatic Discharge) strap attached to the computer case.

B. Wear an air filter mask

A filtered mask would not usually 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 strap would allow the technician to minimize the potential of an electrostatic discharge. However, disconnecting the power source takes a higher priority.



More information:

220-1202, Objective 4.4 - Safety Procedures

<https://professormesser.link/1202040402>

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 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
 - 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 file table, but it doesn't overwrite any data on the drive. With the right software, the previous data could potentially be recovered.

B. Degauss

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 could potentially identify and "undelete" the previous drive data.



More information:

220-1202, Objective 2.9 - Data Destruction

<https://professormesser.link/1202020901>

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 folder the current directory?

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

The Answer: **A.** cd logs

The "cd" command is an abbreviation for "change working directory," and it can be used in Windows or Linux to traverse 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, the results will be filtered for this 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:

220-1202, Objective 1.5 - Windows Command Line Tools

<https://professormesser.link/1202010501>

A41. A system administrator is configuring a server to use eight bootable partitions on a single SSD. Which of the following partition styles would be the best choice for this configuration?

- A.** MBR
 - B.** NTFS
 - C.** diskpart
 - D.** GPT
-

The Answer: D. GPT

The GPT (GUID Partition Table) partition style allows for up to 128 separate bootable partitions.

The incorrect answers:

A. MBR

The MBR (Master Boot Record) partition style provides a maximum of four bootable primary partitions per drive.

B. NTFS

NTFS (NT File System) is a file system designed for Windows computers. Although a system may store files using NTFS, the partition style containing the NTFS file system would determine the maximum number of supported partitions.

C. diskpart

The diskpart utility is a command line option for managing partition styles and bootable configurations. Although diskpart can be used to configure a partition style, the diskpart utility itself is not a partition.



More information:

220-1202, Objective 1.2 - Installing Operating Systems

<https://professormesser.link/1202010201>

A42. A technician is installing a fresh Windows operating system on a file server. Unfortunately, the drive controller in the system is not recognized during the installation process. Which of the following would be the best way to manage this issue?

- A.** Load third-party drivers
 - B.** Restart the system
 - C.** Use a remote network installation
 - D.** Boot from the recovery partition
-

The Answer: **A.** Load third-party drivers

The Windows installation program includes drivers for most hardware devices, but occasionally additional device drivers will need to be added during the installation process.

The incorrect answers:

B. Restart the system

The installation program will still be unable to access the drive controller after a reboot, so restarting the system is an unlikely solution to this issue.

C. Use a remote network installation

Installing Windows across the network can simplify the use of installation media, but it won't provide any additional access to the drive controller.

D. Boot from the recovery partition

Since Windows has not yet been installed on this system, it's unlikely a recovery partition exists. Even if a recovery partition does exist, the installation program will still not have device drivers for the drive controller.



More information:

220-1202, Objective 1.2 - Installing Operating Systems

<https://professormesser.link/1202010201>

A43. A security administrator is concerned a bad actor may use packet analysis to determine a list of web sites visited by their users. Which of the following would prevent this type of reconnaissance?

- A.** Enable full disk encryption
 - B.** Login with multifactor authentication
 - C.** Use a secure DNS
 - D.** Configure the BIOS for secure boot
-

The Answer: **C.** Use a secure DNS

By default, all DNS communication occurs over a non-encrypted session. This doesn't disclose any information from a website, but it can show which fully-qualified domain names are accessed by users. Configuring DNS over HTTPS (DoH) or a similar encryption method can prevent anyone from monitoring this information from packet captures.

The incorrect answers:

A. Enable full disk encryption

Full disk encryption is useful for protecting information on a storage drive, but it does not affect the transfer of data across the network.

B. Login with multifactor authentication

Multifactor authentication (MFA) is used during the authentication process. MFA does not encrypt or protect any type of network communication or DNS queries.

D. Configure the BIOS for Secure Boot

Secure Boot is used during the startup process to ensure the underlying operating system has not been modified by malicious software. Secure Boot does not protect any data sent over the network.



More information:

220-1202, Objective 2.11 - Browser Security

<https://professormesser.link/1202021101>

A44. A user in the sales department is attempting to upgrade the operating system of their smartphone, but the smartphone will not start the installation when selected. Which of the following is the most likely reason for this issue?

- A.** Bluetooth is enabled
 - B.** The smartphone storage is nearly full
 - C.** Rotation lock is disabled
 - D.** The phone is connected to a power source
-

The Answer: **B.** The smartphone storage is nearly full

To upgrade, a smartphone needs enough available storage to download and process the upgrade files. If the storage space is limited, the upgrade will not be processed.

The incorrect answers:

A. Bluetooth is enabled

Bluetooth provides connectivity from a smartphone to other devices, but enabling or disabling Bluetooth does not generally impact the upgrade process of the operating system.

C. Rotation lock is disabled

Disabling rotation lock allows the phone to be easily switched between portrait and landscape modes. The rotation lock is not associated with the upgrade process.

D. The phone is connected to a power source

For an upgrade, it's generally recommended to connect to a power source. However, connecting to a power source would not prevent the operating system upgrade.



More information:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

A45. The hard drive in a macOS desktop has failed and none of the data on the drive is 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.** Mission Control
 - C.** Time Machine
 - D.** Disk Utility
-

The Answer: C. Time Machine

The built-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 recovery utility called "Backup and Restore."

B. Mission Control

Mission Control is an easy way to view all open applications and virtual desktops in macOS.

D. Disk Utility

Disk Utility is a macOS tool for viewing, modifying, and managing storage drives.



More information:

220-1202, Objective 1.8 - macOS System Preferences

<https://professormesser.link/1202010802>

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 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 an open-source license
 - C. The user has installed a personal license
 - D. The software requires a USB key for DRM
-

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

Personally licensed software can be difficult to audit on computers 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 an open-source license

An open-source license would not cause any licensing issues, and many companies will install open-source software on their systems.

D. The software requires a USB key for DRM

Some software requires a USB (Universal Serial Bus) drive to be installed as part of the software's DRM (Digital Rights Management). Although the USB drive might be required to operate the software, it would not cause software to be removed from the system.



More information:



220-1202, Objective 4.6 - Privacy, Licensing, and Policies



<https://professormesser.link/1202040602>

A47. A system administrator is upgrading four workstations from Windows 8.1 to Windows 11. 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.** In-place upgrade
-

The Answer: **C.** Clean install

A clean install of Windows 11 will completely delete the previous operating system and install a new installation of the Windows 11 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 11.

B. Repair installation

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

D. In-place upgrade

Some Windows versions allow an in-place upgrade process to keep user applications and data available after the upgrade is complete. Unfortunately, there are no in-place upgrades available between Windows 8.1 and Windows 11.



More information:

220-1202, Objective 1.2 - Installing Operating Systems

<https://professormesser.link/1202010201>

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 infected with malware, it's important to quarantine the 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 recover 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 the computer is quarantined to prevent the spread of any potential malware.



More information:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

A49. A technician has been called to resolve an issue with a networked laser printer 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 the customer is informed of the plans going forward.

D. Order a printer maintenance kit

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



More information:

220-1202, Objective 4.7 - Communication

<https://professormesser.link/1202040702>

A50. A system administrator is starting a Windows computer, but during startup they receive the message, "One or more services failed to start." Additional reboots result in the same error message. Which of the following would be the best next troubleshooting step?

- A. Check for proper cooling
 - B. Run a hardware diagnostic
 - C. Modify the service permissions
 - D. Rebuild the BCD
-

The Answer: C. Modify the service permissions

Most Windows services start with generic system permissions, but some services may require additional rights. Authentication credentials can be added or changed in the service configuration to provide the correct permissions during startup. The Windows Event Viewer may also provide additional details about the startup error.

The incorrect answers:

A. Check for proper cooling

Poor cooling would result in an overheating system and would most commonly result in a complete shutdown of the system. A thermal issue would not cause a service error, and would probably not be a significant issue until the system has been running for a period of time.

B. Run a hardware diagnostic

Although this issue could potentially be related to a hardware issue, there's no direct evidence of hardware problems in the provided error message. In many cases, problems with a service startup are related to some type of software or permissions issue.

D. Rebuild the BCD

The BCD (Boot Configuration Database) contains information regarding the location of the Windows OS. If the operating system is booting, the BCD is most likely not part of the issue.



More information:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

A51. A system administrator would like all help desk computers to check for anti-virus signature updates every hour during the workday. Which of the following would be the best way to provide this functionality?

- A.** System Configuration
 - B.** Task Scheduler
 - C.** Device Manager
 - D.** Certificate Manager
 - E.** SFC
-

The Answer: **B.** Task Scheduler

The Task Scheduler allows for the automated scheduling of applications and scripts on a Windows computer. The anti-virus update process would be added to the Task Scheduler and would run at predetermined intervals.

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 automated scheduling or application updates.

C. Device Manager

The Device Manager is used to control and manage hardware and device drivers. Device Manager would not provide a scheduling or update function for an anti-virus application.

D. Certificate Manager

The Certificate Manager provides access to the certificates used by the operating system, browser, and any applications. For example, all Active Directory, third-party, and smart card certificates are stored in the Certificate Manager.

E. SFC

SFC (System File Checker) is used to verify the core operating system files are valid. Application updates are not managed through the SFC utility.



More information:

220-1202, Objective 1.4

The Microsoft Management Console

<https://professormesser.link/1202010402>

A52. A workstation on a manufacturing floor is taking much longer to boot than normal. 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 which has been 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 problems might occur after an OS patch update, but it would be unusual for these issues to 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:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

A53. A Windows user is installing a new application, and the installation process 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 in current Windows versions would have the same 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:

220-1202, Objective 2.2 - Windows Security Settings

<https://professormesser.link/1202020203>

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.** WPA3 settings
 - 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 and all traffic between the locations is protected from anyone monitoring the connection. If the VPN link is not active, the remote user will be unable to use any resources at the corporate office.

The incorrect answers:

A. WPA3 settings

WPA3 (Wi-Fi Protected Access 3) is a standard for wireless encryption and security. WPA3 would not be involved in a printing problem across a VPN to a corporate office.

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:

220-1202, Objective 1.7 - Windows Network Connections

<https://professormesser.link/1202010704>

A55. An employee has modified the NTFS permissions on a folder 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 the share permissions include 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 which remote users will have to the resources.



More information:

220-1202, Objective 2.2 - Windows Security Settings

<https://professormesser.link/1202020203>

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 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 which would guarantee all data would be unrecoverable would be to physically destroy the drives.

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 which contained the data. User folder data could possibly be restored with the use of recovery software.



More information:

220-1202, Objective 2.9 - Data Destruction

<https://professormesser.link/1202020901>

A57. A technician was assigned a support ticket with an urgently requested a laptop screen repair. The support team was able to locate a replacement and install a new LCD display in less than 24 hours. The laptop was returned to the user and the user immediately left on a business trip. Which of the following would be the best next step for this repair?

- A.** Order a backup replacement display
 - B.** Update the user's login script
 - C.** Run diagnostics on the original screen
 - D.** Contact the user to verify satisfaction
-

The Answer: **D.** Contact the user to verify satisfaction

Much of the daily processes associated with an IT professional are not technical tasks. Our workloads are often based around communication and interpersonal skills, so keeping the lines of communication open are key. In this example, following up with the customer to check on their satisfaction would be an important last step to this very technical repair.

The incorrect answers:

A. Order a backup replacement display

The display has already been replaced, so it would not be necessary to order additional parts. If the display is damaged again, another replacement can be ordered at that time.

B. Update the user's login script

Login scripts are normally used to initialize a work environment after a user has authenticated. In this example, the screen replacement would not require any updates to the user's login script.

C. Run diagnostics on the original screen

Diagnostics would normally be one of the first steps in order to determine the extent of the damage. Once the display is replaced, a hardware diagnostic would not be necessary.



More information:

220-1202, Objective 4.7 - Communication

<https://professormesser.link/1202040702>

A58. A user has received a pop up message on their computer stating applications on their computer are infected with a virus. A technician has determined the pop up message is a hoax and it 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 the original installation media
-

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 the original installation media

Booting into a command line from the original Windows installation media 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:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

A59. A network administrator needs to manage a switch and a firewall in the local data center. Which of the following would be the best choice for this requirement?

- A.** RDP
 - B.** VPN
 - 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. VPN

A VPN (Virtual Private Network) is used when connecting to a remote site over an encrypted tunnel. In this example, the technician is connecting to devices in a local data center.

D. VNC

VNC (Virtual Network Computing) is a screen sharing technology 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:

220-1202, Objective 4.9 - Remote Access

<https://professormesser.link/1202040901>

A60. A user is using a smartphone at their desk, and they occasionally receive a security warning in the browser. After some additional troubleshooting, the technician determines the security warnings are fake. 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

Fake security warnings would be considered a strong indication of malware. This suspicious activity should be researched further and an anti-malware scan should be used to test 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 fake security warnings.

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 fake security warnings.

D. Remove any paired Bluetooth devices

Bluetooth connections do not generally cause messages to appear on the screen. This almost certainly indicates malware or some other unauthorized process is running on the smartphone.



More information:



220-1202, Objective 3.3



Troubleshooting Mobile Device Security

<https://professormesser.link/1202030301>

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

- A.** Create a login script
 - 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. Create a login script

A login script is often configured in Active Directory to customize the work environment after authentication. In this example, the system isn't booting so there would be no opportunity to run a login script.

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 used to 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:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

A62. A user has opened a help desk ticket relating to desktop alerts randomly appearing throughout the day. Most of the alerts contain information about third-party products and services. Which of the following is the most likely cause of these messages?

- A.** On-path attack
 - B.** Corrupted email database
 - C.** OS update failure
 - D.** Adware
-

The Answer: **D.** Adware

Attackers can make money by forcing advertisements to appear on a user's desktop. This system would need to be recovered from a known good backup to remove the malware.

The incorrect answers:

A. On-path attack

An on-path attack would include a third-party intercepting and potentially modifying network data. In this situation, there's no evidence 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. OS update failure

Although an OS update is certainly important to resolve, missing an update would not cause random advertisements to appear on a user's desktop.



More information:

220-1202, Objective 3.4 - Troubleshooting Security Issues
<https://professormesser.link/1202030401>

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 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 which 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:

220-1202, Objective 4.8 - Scripting Languages

<https://professormesser.link/1202040801>

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. winver
 - 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 which 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. winver

The winver (Windows Version) command line utility will display the "About Windows" dialog box on the screen.

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:

220-1202, Objective 1.5 - Windows Command Line Tools

<https://professormesser.link/1202010501>

A65. A desktop administrator has determined an employee in the corporate office has been using their computer to share copyrighted materials 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 which 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 to create a chain of custody. The computer 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 which 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 which will occur later. The more important task will be to collect the evidence and protect its integrity.



More information:



220-1202, Objective 4.6 - Incident Response

<https://professormesser.link/1202040601>

A66. A system administrator would like to require a specific level of 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. Group Policy allows an administrator to define specific desktop and security policies, such as 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 in the Windows Firewall to allow or prevent access to a specific TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) port. Port security does not define any parameters for password complexity.



More information:

220-1202, Objective 2.2 - Active Directory

<https://professormesser.link/1202020204>

A67. A system administrator is creating a series of shared folders which should not be visible when users browse the network for available 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 share name, so this should not be considered a security feature.

The incorrect answers:

A. . (period)

Adding a period to the end of a Windows share name is not supported.

C. ! (exclamation mark / bang)

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

D. # (hash sign / number sign)

The hash sign is not allowed in a Windows share name.



More information:

220-1202, Objective 1.7 - Windows Network Technologies

<https://professormesser.link/1202010701>

A68. 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. The user has confirmed 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 disabled
 - 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 the user is not connected to one of the available networks, it's most likely 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 disabled

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

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 the wireless radio is active.



More information:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

A69. A desktop administrator is upgrading the video adapter in a 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 to clean. A toner vacuum would not be used during an adapter card upgrade.



More information:

220-1202, Objective 4.4 - Managing Electrostatic Discharge

<https://professormesser.link/1202040401>

A70. A help desk director would like to identify and track computer systems which 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:

220-1202, Objective 4.1 - Asset Management

<https://professormesser.link/1202040102>

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 based only 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 which 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:

220-1202, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1202010601>

A72. A financial management company would like to ensure 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.** UPnP
 - C.** Multi-factor authentication
 - D.** TKIP
 - E.** TACACS
 - F.** Kerberos
 - G.** WPA3
-

The Answer: **C.** Multi-factor authentication, and **G.** WPA3

Multi-factor authentication requires the user to login using two different verification methods, such as a password and a generated token. WPA3 (Wi-Fi Protected Access 3) 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. UPnP

UPnP (Universal Plug and Play) allows network devices to automatically configure and find other network devices. UPnP does not provide wireless encryption or enhanced the authentication process.

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. Kerberos

Kerberos is an authentication protocol commonly associated with Microsoft Windows. Kerberos does not provide additional authentication factors or wireless encryption functionality.



More information:

220-1202, Objective 2.3 - Wireless Encryption
<https://professormesser.link/1202020301>



More information:

220-1202, Objective 2.1 - Logical Security
<https://professormesser.link/1202020103>

A73. A network consulting firm is upgrading the Internet firewalls for a large corporation. The proposal includes a description of the project and the network topology changes required to support the upgrade. The proposal also describes the risks involved with making this upgrade. Which of the following would be the last step in this upgrade?

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

The Answer: **D.** End-user acceptance

The last step of any change control process is to get sign-off from the end users associated with the change.

The incorrect answers:

A. Detailed upgrade plan

Before working through the change control process, it's important to have a detailed explanation of what steps are 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.

B. Backout plan

A backout plan is used to recover from any unexpected or non-working changes. A backout plan would not be the last step in the change control process.

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. This application is not the last step in the change control process.



More information:

220-1202, Objective 4.2 - Change Management
<https://professormesser.link/1202040201>

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 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:

220-1202, Objective 1.5 - Windows Command Line Tools
<https://professormesser.link/1202010501>

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 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 remain in the operating system. 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 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:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

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 battery backup 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:

220-1202, Objective 4.5 - Environmental Impacts

<https://professormesser.link/1202040501>

A77. A financial corporation is deploying laptops to their salespeople in the field. The sales teams require video playback functionality, but the Windows configuration does not include any multimedia utilities. Which of the following would be the most likely reason for these missing utilities?

- A.** Laptops are using Windows N edition
 - B.** Video playback is disabled in the BIOS
 - C.** Laptop hardware does not support video playback
 - D.** The video format is not recognized by the laptop
-

The Answer: **A.** Laptops are using Windows N edition

The N Edition is a version of Windows which does not include the Windows Media Player or any other multimedia utilities. Media players would need to be manually installed after Windows is up and running.

The incorrect answers:

B. Video playback is disabled in the BIOS

The ability to restrict video playback features is not part of a system BIOS. The operating system determines which applications or application features are available in the OS.

C. Laptop hardware does not support video playback

Effectively any laptop would be able to provide playback of video content, so it would be very unusual for there to be a hardware issue with the laptops and multimedia content.

D. The video format is not recognized by the laptop

This question does not mention any issues with the laptops during the video playback process, so an issue with the video format would not be the most likely reason for the missing media utilities.



More information:

220-1202, Objective 2.8 - Mobile Device Security

<https://professormesser.link/1202020801>

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:

220-1202, Objective 1.4 - The Microsoft Management Console
<https://professormesser.link/1202010402>

A79. While using a Windows laptop during presentations, a company vice president has reported her system is interrupting the meeting with system notifications from the browser, PDF reader, the Microsoft Store, and other applications. Which of the following would be the best way to address this issue?

- A.** Use a different laptop for presentations
 - B.** Run the presentation software as Administrator
 - C.** Enable Airplane mode while presenting
 - D.** Disable notifications while specific applications are running
-

The Answer: **D.** Disable notifications while specific applications are running

Windows provides numerous configuration options for operating system notifications, including the ability to individually manage notifications by application, or to enable or disable all notifications. Windows also has an option to disable notifications while certain applications are running.

The incorrect answers:

A. Use a different laptop for presentations

Using a separate laptop just for presentations would be costly and unnecessary. The notification options can be easily managed through the System Control Panel applet.

B. Run the presentation software as Administrator

Running the presentation with elevated rights and permissions would not prevent or suppress the operating system notification prompts.

C. Enable Airplane mode while presenting

Airplane mode would prevent the use of Wi-Fi or Bluetooth connections during the presentation, but it would also prevent the use of network services during the meeting. This option would also not prevent the unwanted operating system notifications from appearing.



More information:

220-1202, Objective 3.4 - Troubleshooting Security Issues
<https://professormesser.link/1202030401>

A80. A system administrator needs to upgrade a training room of twenty systems to the latest Windows version. Which of the following would be the most efficient method of performing this upgrade process?

- A.** Recovery partition
 - B.** Remote network installation
 - C.** Repair installation
 - D.** USB key
-

The Answer: **B.** Remote network installation

A single network server can provide access for simultaneous upgrades. With additional customization, the upgrade process can be completely hands-off and can execute on all systems at the same time.

The incorrect answers:

A. Recovery partition

A recovery partition does not generally provide a method of upgrading an operating system, and it requires each system to be accessed locally during the installation.

C. Repair installation

A repair installation does not upgrade an operating system, and it usually requires intervention on each system to complete the repair process.

D. USB key

USB media is an efficient method of accessing a large number of files, but it either requires the administrator to upgrade one system at a time or it requires twenty separate USB keys to perform the upgrade.



More information:

220-1202, Objective 1.2 - Installing Operating Systems

<https://professormesser.link/1202010201>

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 the computer, 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 network as soon as malware is suspected. The system would not need to be quarantined after the malware has been successfully removed.



More information:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

A82. An employee at a company is responsible for determining the correct access controls for each user, manage the authentication process, and track all access to network resources. Which of the following would best describe this employee's job function?

- A. PAM
 - B. DLP
 - C. MDM
 - D. IAM
-

The Answer: D. IAM

IAM (Identity Access Management) focuses on identity lifecycle management, where every network entity gets a digital identity. The objective of IAM is to prevent unauthorized access by giving the right permissions to the right people at the right time.

The incorrect answers:

A. PAM

PAM (Privileged Access Management) is a broad approach to managing access. PAM focuses on centralizing password management, automating access processes, and managing access and reporting for each user.

B. DLP

DLP (Data Loss Prevention) describes strategies and technologies for preventing the unintended or unauthorized disclosure of sensitive information. DLP is not directly associated with the management of access controls.

C. MDM

An MDM (Mobile Device Manager) is a centralized system for managing smartphones, tablets, and other mobile devices in the enterprise. The MDM is also used to apply security controls and manage app use.



More information:

220-1202, Objective 2.1 - Authentication and Access

<https://professormesser.link/1202020104>

A83. 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. While testing other website connections on the computer, the technician finds 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 would reasonably believe the pop-up windows indicated a malware infection. Given the available answers, the only one which 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 Safe Mode would provide access to the third-party website.

D. Modify the browser's proxy settings

There's no evidence 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:

220-1202, Objective 3.4 - Troubleshooting Security Issues

<https://professormesser.link/1202030401>

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.** Restrict log-in times for the partner account
 - 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.** Restrict log-in times for the partner account

One way to prevent unauthorized access is to limit the times when access to the server is available. Restricting the log-in times will limit all access, including log-in attempts by unauthorized individuals.

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

One concern with this server is access by unknown third-parties from the partner's network. A weekly anti-virus scan is a useful best practice, but it would not provide any additional log-in restrictions.



More information:

220-1202, Objective 2.7 - Security Best Practices

<https://professormesser.link/1202020701>

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
 - C.** dig
 - 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

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

C. dig

The dig (Domain Information Groper) command is used to query a DNS (Domain Name System) server for IP address or fully-qualified domain name details. The dig command does not provide any additional permissions.



More information:

220-1202, Objective 1.9 - Linux Commands Part 1

<https://professormesser.link/1202010902>

A86. A user is connecting their laptop to an external monitor and keyboard, but the laptop goes into sleep mode if the laptop screen is shut. Which of the following utilities can be used to keep the laptop running when the lid is closed?

- A.** Power Options
 - B.** Device Manager
 - C.** Personalization
 - D.** User Accounts
-

The Answer: **A.** Power Options

The Control Panel's Power Options provide configuration settings for the sleep button, the power button, and the options when closing the lid of a laptop computer.

The incorrect answers:

B. Device Manager

The Device Manager is used to install or update device drivers on a Windows computer. The Device Manager does not manage the power configuration options.

C. Personalization

The Windows Settings include Personalization options for changing the way Windows looks and feels. This includes colors, wallpaper, the lock screen, and other user interface settings.

D. User Accounts

Account name, picture, password, and certificate information can be found in the Control Panel's User Accounts applet. The User Accounts setting does not provide any configuration options for the laptop screen.



More information:

220-1202, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1202010601>

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. Secure management access
 - D. DHCP reservation
 - E. IP filtering
-

The Answer: E. IP filtering

IP (Internet Protocol) address filtering can be configured to allow or deny access to the network based on the IP address of the network adapter. Given the available options, IP 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 prevent the display of 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 traffic 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. Secure management access

Many SOHO routers include options for preventing management access from external networks, and for encrypting the connection to the management interface. However, securing the management access would not prevent access to the network by other devices.

D. DHCP reservation

A DHCP (Dynamic Host Configuration Protocol) reservation is used to associate the MAC (Media Access Control) address of a device to a specific IP address. A DHCP reservation does not limit access on a wireless network.



More information:

220-1202, Objective 2.10 - Securing a SOHO Network

<https://professormesser.link/1202021001>

A88. A company has installed a Windows system in the conference room for use during meetings. However, the system has not received any recent OS updates and will no longer connect to the corporate network due to missing security patches. Which of the following would be the most likely reason for this issue?

- A.** BIOS administrator password is enabled
 - B.** No users are actively logged in
 - C.** Firewall is filtering traffic
 - D.** Guest accounts are disabled
-

The Answer: **C.** Firewall is filtering traffic

Operating system updates are normally downloaded from a server across the network, so any restrictions or filtering of the network traffic flows will prevent updates of the operating system and applications.

The incorrect answers:

A. BIOS administrator password is enabled

The BIOS administrator password prevents any changes to the BIOS configuration. The Windows operating system does not require access to the BIOS to install patches and updates.

B. No users are actively logged in

Windows runs many different services on a device. The update process runs as one of these services, and the process does not require a specific user login name or authentication to update the OS.

D. Guest accounts are disabled

The best practice for guest accounts is to always disable them, and disabling these accounts would not prevent patches and updates from being downloaded and installed.



More information:

220-1202, Objective 3.4 - Troubleshooting Security Issues

<https://professormesser.link/1202030401>

A89. A company is deploying laptops to all of their field sales teams. The company is concerned about protecting the security of data if the laptop is stolen or misplaced. Which of the following would be the best way to address this concern?

- A.** Multifactor authentication
 - B.** Strong password policies
 - C.** Unique device certificates
 - D.** Data-at-rest encryption
-

The Answer: **D.** Data-at-rest encryption

Data-at-rest encryption is associated with all data stored on the laptop's SSD or hard drives. If the laptop is stolen or misplaced, all of the data on the storage drive would be protected from unauthorized users.

The incorrect answers:

A. Multifactor authentication

Multifactor authentication provides additional security during the login process, but it does not create any additional protections for data on a storage drive.

B. Strong password policies

All password policies should require strong passwords, but those passwords do not provide any data security for information stored on a laptop or mobile device.

C. Unique device certificates

Many organizations will install device certificates on their laptops to assist with the authentication and verification processes when the laptop is in the field. The certificate ensures the device is an authorized company laptop, but it does not provide any additional security for any stored files.



More information:

220-1202, Objective 2.7 - Security Best Practices

<https://professormesser.link/1202020701>

A90. A company has discovered a recent data breach, and this breach appears to have originated through a vulnerability introduced with a software upgrade. The vulnerability was added by the attacker at the source and distributed to all customers who performed the upgrade. Which of the following would best describe this attack type?

- A.** Supply chain attack
 - B.** Insider threat
 - C.** Business email compromise
 - D.** On-path attack
-

The Answer: **A.** Supply chain attack

A supply chain attack takes advantage of the trust from a supplier and uses this trust to install or embed security vulnerabilities. A software vulnerability originally installed into the source code by the attacker and distributed to all customers would be an attack to the supply chain.

The incorrect answers:

B. Insider threat

An insider threat would be an attack from an employee or someone trusted internally in the company. In this example, the attacker was a third-party who was not part of the software company or the customer.

C. Business email compromise

A business email compromise uses email as the primary method of attack. In this example, the attack used a software upgrade process to embed a vulnerability into the network and email was not used as the delivery or attack method.

D. On-path attack

An on-path attack requires the attacker to physically act in the middle of an active communications path. In this example, the attacker embedded their code and was not actively part of the code distribution.



More information:

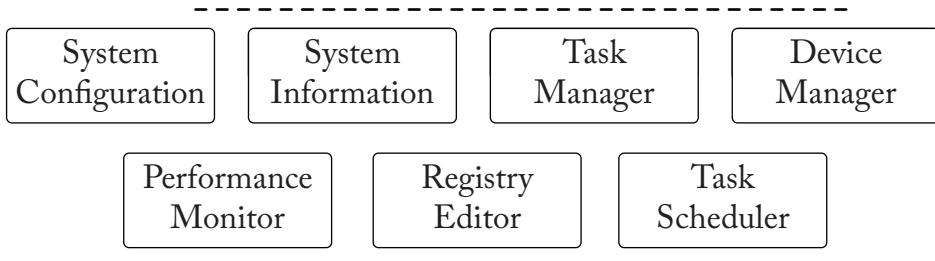
220-1202, Objective 2.5 - Supply Chain Attacks

<https://professormesser.link/1202020510>

Practice Exam B

Performance-Based Questions

- B1. A system administrator is troubleshooting complaints of a performance problem on a Windows laptop. Specify the best Windows utility to accomplish the following tasks.



Task 1:

The first step is to determine the current status of the system. Select a utility to view the real-time display of CPU utilization, memory usage, disk access, network utilization, and more.

Task 2:

There were no obvious resource issues identified in the previous step, and the administrator believes the problem may be intermittent. Use a Windows utility to gather long-term information over a 24-hour period.

Task 3:

The long-term analysis shows high CPU utilizations when a specific application is running. This issue may be related to a known bug. Launch a utility to view the Windows and BIOS versions of this laptop.

Task 4:

After updating Windows, the performance issues appear to be resolved. Going forward, the administrator would like to automatically perform a daily check to install any pending updates.

Answer Page: 167

- B2.** A network administrator is troubleshooting an intermittent Internet link outage to a server at 8.8.8.8. The administrator believes the outage is occurring on one of the WAN connections between locations. Use a Windows network utility to identify the router closest to the outage.



Answer Page: 169

.....

- B3.** A system administrator is updating the scripts used by different processes and services. Select the best scripting language the administrator should choose for each task. Not all scripting languages will be used.

.bat

.ps1

.vbs

.sh

.js

.py

For onboarding, create an Active Directory account and automatically add the user to the necessary groups

Change a webpage to show the flag of the visitor's country based on their IP address

Use a single script to backup log files in Windows, Linux, and macOS

Analyze data in an Excel spreadsheet and convert all measurements to metric values

Each night, four load-balanced Linux web servers should be restarted in series

Answer Page: 170

- B4.** Select the Windows 11 Editions which include the following features.
Multiple Windows Editions may be selected for a single feature.

| | | | |
|------------------------|------|-----|------------|
| Workgroup support only | Home | Pro | Enterprise |
| Domain support | Home | Pro | Enterprise |
| Supports 6 TB of RAM | Home | Pro | Enterprise |
| BitLocker encryption | Home | Pro | Enterprise |
| Remote Desktop Service | Home | Pro | Enterprise |

Answer Page: 172

- B5.** A system administrator is concerned a Windows system may contain logical file system errors. Scan and repair any logical file system errors from the Windows command line.



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window is running in administrator mode, indicated by the "Administrator" label in the title bar. The command prompt itself shows the path "C:\WINDOWS\system32>". The window has standard Windows-style borders and a scroll bar on the right side.

Answer Page: 173

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.** Perform a regular format
- B.** Run a defragmentation
- C.** Connect the laptop to the Windows Domain
- D.** Delete the \Users folder

Quick
Answer: **165**

The Details: **175**

B7. A company has just performed annual laser printer maintenance, and has accumulated hundreds of used toner cartridges. Which of the following would be the best way to dispose of the old cartridges?

- A.** Take to a hazardous waste facility
- B.** Send in bulk to the local landfill
- C.** Separate the parts and dispose of normally
- D.** Contract with an incineration company

Quick
Answer: **165**

The Details: **176**

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: **165**

The Details: **177**

B9. A macOS server administrator needs a backup system to 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.** Spotlight
- C.** Spaces
- D.** Time Machine

Quick
Answer: **165**

The Details: **178**

B10. Why would a technician use an ESD strap?

- A.** Protect electronic parts from extreme heat
- B.** Keep electronic parts dry and free from moisture
- C.** Prevent damage from static electricity
- D.** Protect computer parts from dust

Quick
Answer: **165**

The Details: **179**

B11. A technician needs to uninstall a video editing utility from a macOS laptop. Which folder would be the most likely location of this utility?

- A.** /Program Files
- B.** /Applications
- C.** /Library
- D.** /Users

Quick
Answer: **165**

The Details: **180**

B12. 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: **165**

The Details: **181**

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.** diskpart
- C.** robocopy
- D.** dir

Quick
Answer: **165**

The Details: **182**

B14. A user runs a corporate app on their smartphone which 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.** Charge the smartphone battery
- D.** Check the cloud storage resource usage

Quick
Answer: **165**

The Details: **183**

B15. A system administrator is analyzing a problem with a USB flash drive on a Windows 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: **165**

The Details: **184**

B16. A user is reporting 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 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: **165**

The Details: **185**

B17. A technician has been asked to power down and store a server which 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: **165**

The Details: **186**

B18. 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: **165**

The Details: **187**

B19. Which of the following features would be found in Windows 11 Pro but not in Windows 11 Home?

- A. 32-bit and 64-bit versions
- B. Domain access
- C. RDP client
- D. Windows Workgroup

Quick
Answer: **165**

The Details: **188**

B20. A medical research company is using laptop computers when visiting testing centers. The IT security team is concerned about a 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 application
- C.** Full disk encryption
- D.** Biometric authentication
- E.** Cable lock

Quick
Answer: **165**

The Details: **189**

B21. A security administrator is installing a new VPN connection for remote users. The administrator would like all users to authenticate with their Windows Active Directory credentials. Which of the following technologies would provide this functionality?

- A.** RADIUS
- B.** WPA3
- C.** TKIP
- D.** AES

Quick
Answer: **165**

The Details: **190**

B22. A mobile user is using apps on their smartphone for most business tasks. To ensure 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: **165**

The Details: **191**

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: **165**

The Details: **192**

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: **165**

The Details: **193**

B25. 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: **165**

The Details: **194**

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.** Remote network installation
- C.** Clean install
- D.** Repair installation

Quick
Answer: **165**

The Details: **195**

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 customers can never connect to the company network. Which of the following should be configured on this network?

- A.** Install a new access point for company devices
- B.** Configure WPA3 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: **165**

The Details: **196**

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: **165**

The Details: **197**

B29. A company's shipping department maintains ten different computers for printing shipping labels and for tracking outgoing shipments. All of the systems are displaying an error when they 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: **165**

The Details: **198**

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.** Assign an expiration date to the auditor accounts
- C.** Remove the auditor accounts from all Windows groups
- D.** Require two-factor authentication for the auditor accounts

Quick
Answer: **165**

The Details: **199**

B31. A manufacturing company is donating some older computers to a local charity. Which of the following should be done to ensure 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: **165**

The Details: **200**

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 the building 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: **165**

The Details: **201**

B33. A desktop administrator is troubleshooting an older computer which 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.** xcopy
- E.** winver

Quick
Answer: **165**

The Details: **202**

B34. A user is receiving alerts on their desktop computer stating, "Access to this PC has been blocked for security reasons." A technician has determined this message was not created by the company's security software. Which of the following would be the best next step in this troubleshooting process?

- A.** Update the desktop computer operating system
- B.** Check the certificate of the corporate web server
- C.** Restart the desktop computer
- D.** Run an anti-malware utility

Quick
Answer: **165**

The Details: **203**

B35. A system administrator has inadvertently installed a Trojan horse which 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: **165**

The Details: **204**

B36. A technician has created a Windows image which can be used across all of the computers in a test lab. Which of the following would be the best way to deploy these images?

- A. Clean install
- B. Remote network installation
- C. Repair installation
- D. Bootable USB

Quick
Answer: **165**

The Details: **206**

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: **165**

The Details: **207**

B38. A data center manager would like to ensure any potential 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. Battery backup
- C. Air filter mask
- D. ESD mat

Quick
Answer: **165**

The Details: **208**

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.** Shoulder surfing

Quick
Answer: **165**

The Details: **209**

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 Restore
- B.** Educate the end-user
- C.** Quarantine the computer
- D.** Boot to Safe Mode

Quick
Answer: **165**

The Details: **210**

B41. A user would like to encrypt a small group of files in a shared folder without modifying other files on the drive. Which of the following would be the best way to accomplish this?

- A.** EFS
- B.** Save the files with Administrator rights
- C.** BitLocker
- D.** Save the files with a dollar sign at the end of the filename

Quick
Answer: **165**

The Details: **211**

B42. Which of the following partition types limit a Windows installation to a maximum partition size of 2 TB?

- A.** FAT32
- B.** GPT
- C.** APFS
- D.** MBR

Quick
Answer: **165**

The Details: **212**

B43. A user in the engineering department needs to use some applications written for Windows, but also needs to use applications designed for Linux. Which of the following would be the best way to provide access to these applications?

- A.** Assign the user multiple computers
- B.** Boot the operating systems from two removable USBs
- C.** Configure the user's PC for multiboot
- D.** Compile the Linux applications in Windows

Quick
Answer: **165**

The Details: **213**

B44. A help desk technician has been tasked with rebuilding an email server which recently crashed. Which of the following would be the best source for the information required to reconstruct this system?

- A.** Compliance report
- B.** Acceptable use policies
- C.** Network topology map
- D.** Knowledge base

Quick
Answer: **165**

The Details: **214**

B45. The employees of a company have direct access to applications and databases from their desktop computers. If the employees are using the company wireless network or the conference room, connectivity is only available after authenticating through a VPN. Which of the following would best describe this policy?

- A.** Multifactor authentication
- B.** Group Policy
- C.** Least privilege
- D.** Zero trust

Quick
Answer: **165**

The Details: **215**

B46. A user has called the help desk to get assistance with random blue screens on their Windows laptop. The technician finds CPU utilization is constantly high, and many network sites are unavailable or only load half of the site content. The user mentions 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: **165**

The Details: **216**

B47. A technician is troubleshooting an issue with an iOS tablet randomly restarting during normal use. A check of the device shows 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: **165**

The Details: **217**

B48. A system administrator needs to modify a file in the \Windows\Installer directory, but the folder doesn't appear in the list of available files. 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

Quick
Answer: **165**

The Details: **218**

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

Quick
Answer: **165**

The Details: **219**

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

Quick
Answer: **165**

The Details: **220**

B51. An executive has a laptop which runs very slowly after login and continues running slowly throughout the day. The user has complained certain applications cannot be started and others will randomly crash. A check of the laptop shows 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: **165**

The Details: **221**

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.** VPN
- B.** VNC
- C.** SSH
- D.** RDP

Quick
Answer: **165**

The Details: **222**

B53. A technician would like to modify a configuration in a user's UEFI BIOS, but the system will not provide a BIOS configuration hotkey after shutting down and powering on the computer. Which of the following would be the best way to address this issue?

- A.** Change the File Explorer Options
- B.** Modify the Indexing Options
- C.** Turn off Fast Startup
- D.** Start the computer in Safe Mode
- E.** Modify the Ease of Access settings

Quick
Answer: **165**

The Details: **223**

B54. A user has noticed their mouse arrow has been moving around the screen when they are not touching the mouse. The user has watched the mouse opening 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: **165**

The Details: **224**

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 risk analysis wasn'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

Quick
Answer: **165**

The Details: **225**

B56. A user receives a browser security alert on his laptop when visiting any website which 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

Quick
Answer: **165**

The Details: **226**

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 which work in the background
- F.** Perform a soft reset

Quick
Answer: **165**

The Details: **227**

B58. A system administrator would like to create a Windows distribution which can automatically configure itself to connect to the corporate domain and automatically configure individual user email settings. Which of the following would be the best choice for this requirement?

- A.** Zero-touch deployment
- B.** Recovery partition installation
- C.** Image deployment
- D.** In-place upgrade

Quick
Answer: **165**

The Details: **228**

- B59.** A user in the accounting department has installed a new application for the upcoming tax year. Although the current application worked perfectly, the newer application runs significantly slower. Which of the following should be the first troubleshooting step?
- A.** Roll back to the previous application
 - B.** Run a repair installation
 - C.** Verify the requirements for the new application
 - D.** Perform a system file check
- B60.** A macOS user needs to protect all of the data on their laptop if the laptop is stolen or lost. Which of the following would be the best choice for this requirement?
- A.** Spaces
 - B.** Mission Control
 - C.** FileVault
 - D.** Keychain
- B61.** A data center manager is installing a new access door which will require multi-factor authentication. Which of the following should be used to meet this requirement? (Select TWO)
- A.** Cabinet locks
 - B.** Key fobs
 - C.** Privacy filter
 - D.** Palmprint scanner
 - E.** USB lock
 - F.** Cable lock

B62. A company is deploying a new set of laptops for field service technicians who travel and work at customer locations. The IT department has been asked to create a secure authentication factor for a minimal cost. Which of the following would be the best choice for this security requirement?

- A.** Retina scanner
- B.** TOTP app
- C.** Keyfob
- D.** Magnetometer

Quick
Answer: **165**

The Details: **232**

B63. An 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: **165**

The Details: **233**

B64. The clock on an executive's Windows laptop has consistently been losing time and is behind by a few minutes at the end of the week. The executive uses this laptop to monitor an assembly line and needs the time and date to be as accurate as possible. Which of these would be the best way to address this issue?

- A.** Create a login script to update the date and time
- B.** Configure an NTP server
- C.** Set the clock for a different time zone
- D.** Replace the laptop batteries

Quick
Answer: **165**

The Details: **234**

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 internal data center door? (Select TWO)

- A.** Biometric lock
- B.** ACL
- C.** Bollard
- D.** Additional lighting
- E.** Motion sensor
- F.** Access control vestibule

Quick
Answer: **165**

The Details: **235**

B66. An administrator is troubleshooting an error message which 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 Monitor to view operational data
- B.** Check the Event Viewer logs
- C.** View the hardware settings in Device Manager
- D.** Disable unneeded background processes in Services

Quick
Answer: **165**

The Details: **236**

B67. Four users in the accounting department have received similar emails asking for payment of an outstanding invoice and a link to a third-party payment site. The emails contains purchase information which appears to be correct, but additional research shows the invoice numbers are not valid. Which of the following would best describe this attack type?

- A.** Spear phishing
- B.** Denial of service
- C.** Shoulder surfing
- D.** Evil twin

Quick
Answer: **165**

The Details: **237**

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

Quick
Answer: **165**

The Details: **238**

B69. Which of these describes a free, open-source operating system?

- A.** macOS
- B.** Linux
- C.** Windows
- D.** iOS

Quick
Answer: **165**

The Details: **239**

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

Quick
Answer: **165**

The Details: **240**

B71. A network administrator has a report showing a single user with numerous visits to a website. This website is known to violate 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: **165**

The Details: **241**

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: **165**

The Details: **242**

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: **165**

The Details: **243**

B74. An employee used their tablet to take pictures of the company's newest product. 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.** Cloud storage
- B.** USB flash drive use
- C.** Application updates
- D.** Deleted email messages

Quick
Answer: **165**

The Details: **244**

B75. A manufacturing company in the United States sells monthly subscriptions from their website. Which of the following regulated data types would be the MOST important to manage?

- A.** Personal government-issued information
- B.** Credit card transactions
- C.** Healthcare data
- D.** Software license terms

Quick
Answer: **165**

The Details: **245**

B76. A user is traveling to a conference, and they would like to be sure any messages sent from their phone during the event remain private while using the event's wireless network. 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: **165**

The Details: **246**

B77. Last week, a computer on the manufacturing floor was upgraded from 8 GB of RAM to 16 GB. Since the upgrade, the system has rebooted itself randomly every few hours. Which of the following would be the best next troubleshooting step?

- A.** Run Windows Update
- B.** Perform a hardware diagnostic
- C.** Upgrade the BIOS to the latest version
- D.** Replace the storage drive

Quick
Answer: **165**

The Details: **247**

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 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 battery backup
- C.** Create separate file-level backups
- D.** Perform occasional recovery tests

Quick
Answer: **165**

The Details: **248**

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 features provides access to these settings?

- A.** Internet Options
- B.** Devices and Printers
- C.** Network and Sharing Center
- D.** System

Quick
Answer: **165**

The Details: **249**

B80. An Android phone user is traveling internationally and would like to avoid overage charges for using too much cellular data while overseas. Which of the following would be the best way to control data access?

- A. Install a VPN client
- B. Remove all apps with high data requirements
- C. Enable data usage notifications
- D. Connect exclusively through a cellular hotspot

Quick
Answer: **165**

The Details: **250**

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: **165**

The Details: **251**

B82. A system administrator is installing a new video editing application on a user's workstation from a USB flash drive. 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 share 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: **165**

The Details: **252**

B83. A user would like to install an image and photo editing program on their home computer, but they would prefer an application without a monthly subscription. Which of the following would be the best licensing option for this requirement?

- A. Open-source
- B. Corporate
- C. Personal
- D. DRM

Quick
Answer: **165**

The Details: **253**

B84. A system administrator is troubleshooting an application issue. 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: **165**

The Details: **254**

B85. An administrator is troubleshooting a desktop computer experiencing a reboot issue. 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: **165**

The Details: **255**

B86. A user has downloaded a browser add-on which assists with new car purchases. During the installation, the Windows UAC is requesting permissions to continue with the install. Which of these is most likely?

- 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: **165**

The Details: **256**

B87. A technician is working on many different terminal sessions on their screen from different servers. The technician has also used different authentication credentials on each server. Which of the following would be the best way to display the login name associated with each terminal session?

- A.** winver
- B.** nslookup
- C.** whoami
- D.** net use

Quick
Answer: **165**

The Details: **257**

B88. A system administrator needs a way to deploy new smartphone configurations across four different user groups. Each group will require a different set of email and security configurations. Which of the following would be the best way to setup these smartphones?

- A.** Assign configuration profiles for each group
- B.** Restore all smartphones from cloud backups
- C.** Provide customized instructions for each user
- D.** Assign separate support teams for each group

Quick
Answer: **165**

The Details: **258**

B89. A desktop administrator is troubleshooting an error which 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

Quick
Answer: **165**

The Details: **259**

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: **165**

The Details: **260**

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. B | 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

Performance-Based Answers

- B1.** A system administrator is troubleshooting complaints of a performance problem on a Windows laptop. Specify the best Windows utility to accomplish the following tasks.

Task 1:

Task
Manager

The first step is to determine the current status of the system. Select a utility to view the real-time display of CPU utilization, memory usage, disk access, network utilization, and more.

The Task Manager is a great place to start the troubleshooting process. The Task Manager shows real-time information about system performance, and it's relatively easy to quickly find high levels of utilization.

Task 2:

Performance
Monitor

There were no obvious resource issues identified in the previous step, and the administrator believes the problem may be intermittent. Use a Windows utility to gather long-term information over a 24-hour period.

If there's a need to monitor over a longer timeframe, then Performance Monitor would be the right choice. Performance Monitor can gather long-term statistics of OS metrics, set alerts and automated actions, store statistics, and display built-in reports.

Task 3:

System
Information

The long-term analysis shows high CPU utilizations when a specific application is running. This issue may be related to a known bug. Launch a utility to view the Windows and BIOS versions of this laptop.

The System Information utility provides an easy way to view a summary of system information, hardware resources, components, software, and more.

Task 4:

Task Scheduler

After updating Windows, the performance issues appear to be resolved. Going forward, the administrator would like to automatically perform a daily check to install any pending updates.

The Windows Task Scheduler allows the user or administrator to run scripts or applications at designated times. This would be a good option for automatically checking for updates every 24 hours.

Other (unused) Windows utilities:

System Configuration:

The System Configuration utility provides an easy method of configuring Windows startup parameters, boot options, and service availability after a reboot.

Device Manager:

Device Manager centralizes the management of Windows device drivers into a single utility. Hardware can be installed, uninstalled, and managed from this all-in-one utility.

Registry Editor:

The Registry contains important configuration parameters for almost every aspect of the Windows operating system.



More information:

220-1202, Objective 1.4

The Microsoft Management Console

<https://professormesser.link/1202010402>

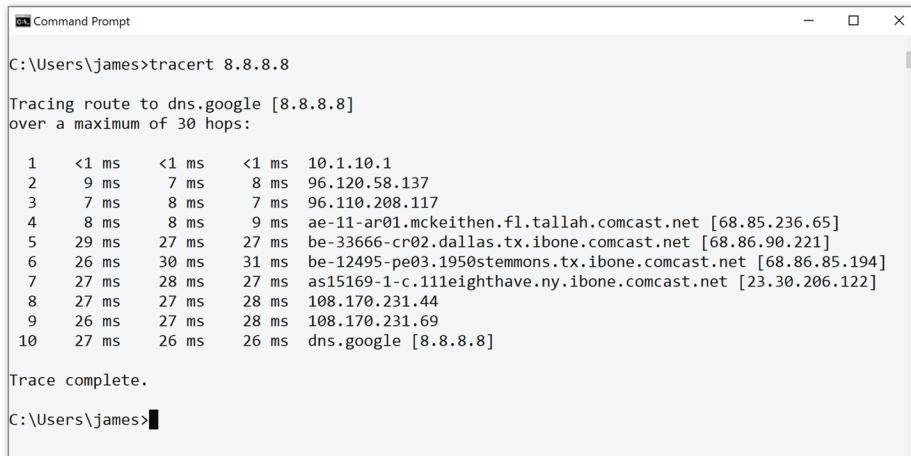


More information:

220-1202, Objective 1.4 - Additional Windows Tools

<https://professormesser.link/1202010403>

- B2.** A network administrator is troubleshooting an intermittent Internet link outage to a server at 8.8.8.8. The administrator believes the outage is occurring on one of the WAN connections between locations. Use a Windows network utility to identify the router closest to the outage.



```
Command Prompt

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.111eighthave.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 tracert output will show the last hop before the faulty link.



More information:

220-1202, Section 1.5 - The Windows Network Command Line

<https://professormesser.link/1202010502>

- B3.** A system administrator is updating the scripts used by different processes and services. Select the best scripting language the administrator should choose for each task. Not all scripting languages will be used.

.ps1

For onboarding, create an Active Directory account and automatically add the user to the necessary groups

PowerShell (.ps1) is a Windows-only scripting environment which extends the functionality of the traditional Windows command line. PowerShell is commonly used at the command prompt to enable the automation of internal Windows and Active Directory functions.

.js

Change a webpage to show the flag of the visitor's country based on their IP address

JavaScript (.js) is used on many web sites to enhance the functionality inside of a user's browser. This can be used for automation, tracking, interactivity features, and to extend the functionality of the browser.

.py

Use a single script to backup log files in Windows, Linux, and macOS

Python (.py) is a scripting language which can handle almost anything, including a number of tasks in this list. However, Python is the best fit for a scripting language for inter-operating with other operating systems, including devices across the network.

.vbs

Analyze data in an Excel spreadsheet and convert all measurements to metric values

VBScript, (.vbs) (Microsoft Visual Basic Scripting Edition) can be used for many Windows-related scripting purposes, and one of the most common is to automate the functionality of Microsoft Office applications.

.sh

Each night, four load-balanced Linux web servers
should be restarted in series

A shell script (.sh) 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 powerful automation options.

Unused option:

.bat

A batch file (.bat) commonly runs in the console or command line of a Windows device, and it can automate the same processes a user would perform manually at the Windows command prompt.



More information:

220-1202, Objective 4.8 - Scripting Languages

<https://professormesser.link/1202040801>

- B4.** Select the Windows 11 Editions which include the following features.
Multiple Windows Editions may be selected for a single feature.

Workgroup support only

Home

Windows Workgroups provide a way to manage access to multiple devices on a small network. This is often used in a SOHO environment where large-scale management is not required. Windows Home edition only includes support for Workgroups and cannot connect to a Windows Domain.

Domain support

Pro

Enterprise

Connecting to a Windows Domain isn't commonly required on a Windows Home computer, so this feature is only found in Windows 11 Pro and higher editions.

Supports 6 TB of RAM

Enterprise

The maximum RAM supported for Windows 11 Home is 128 GB, the Pro edition supports 2 TB of RAM as the maximum, and the Enterprise edition of Windows 11 supports a maximum of 6 TB of memory.

BitLocker encryption

Pro

Enterprise

BitLocker encrypts the entire volume in the Windows operating system, but this feature is not part of the Home edition of Windows 11. The Home edition includes a more limited full disk encryption feature called "Device Encryption" and it integrates with the user's Microsoft account in the cloud.

Remote Desktop Service

Pro

Enterprise

The service used by Remote Desktop is not available in Windows 11 Home Edition. The client used to connect to a Remote Desktop service is available on many different operating systems, including all Windows editions.



More information:

220-1202, Objective 1.3 - Windows Features

<https://professormesser.link/1202010302>

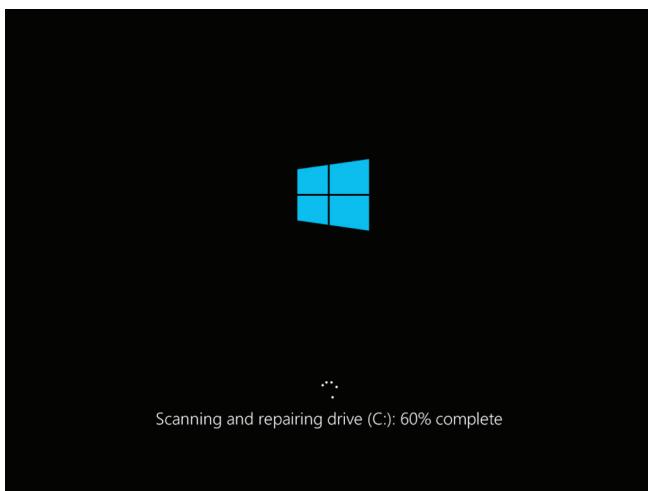
- B5.** A system administrator is concerned a Windows system may contain logical file system errors. Scan and repair any logical file system errors from the Windows command line.
-

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.

In this example, the administrator would run this from the command line:

```
chkdsk /f
```

The scanning and repair process is often completed during a reboot:



More information:

220-1202, 1.5 - Windows Command Line Tools
<https://professormesser.link/1202010501>

Practice Exam B

Multiple Choice Detailed Answers

- 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. Perform a regular format
 - B. Run a defragmentation
 - C. Connect the laptop to the Windows Domain
 - D. Delete the \Users folder
-

The Answer: A. Perform a regular format

A regular format in Windows will overwrite each sector with zeros. Once this information is overwritten, it cannot be obtained or reconstructed.

The incorrect answers:

B. Run a defragmentation

Although a defragmentation can overwrite some data, there's no guarantee 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 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:

220-1202, Objective 2.9 - Data Destruction

<https://professormesser.link/1202020901>

B7. A company has just performed annual laser printer maintenance, and has accumulated hundreds of used toner cartridges. Which of the following would be the best way to dispose of the old cartridges?

- A.** Take to a hazardous waste facility
 - B.** Send in bulk to the local landfill
 - C.** Separate the parts and dispose of normally
 - D.** Contract with an incineration company
-

The Answer: **A.** Take to a hazardous waste facility

The toner in a laser printer cartridge can be harmful, so it's important to dispose of the cartridges at a local hazardous waste facility.

The incorrect answers:

B. Send in bulk to the local landfill

The harmful components of a laser printer cartridge require special handling during disposal. Most MSDS (Material Safety Data Sheet) documentation requires disposal of laser printer cartridges at a hazardous waste facility.

C. Separate the parts and dispose of normally

There's no need to separate the parts of a toner cartridge, and it would probably create a large mess and put toner particles into the air. Even if the cartridges were dismantled, they would not be thrown out with the normal trash.

D. Contract with an incineration company

Toner cartridges should not be incinerated, and instead should be properly disposed of at a local hazardous waste utility.



More information:

220-1202, Objective 4.5 - Environmental Impacts

<https://professormesser.link/1202040501>

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:

220-1202, Objective 1.5 - The Windows Network Command Line

<https://professormesser.link/1202010502>

B9. A macOS server administrator needs a backup system to 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.** Spotlight
 - 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. Spotlight

Spotlight is the built-in search feature in macOS. Spotlight does not provide any backup or restore capabilities.

C. Spaces

The Spaces utility can be used in macOS to create multiple desktops and separate work "spaces" which can be used independently of each other.



More information:

220-1202, Objective 1.8 - macOS System Preferences

<https://professormesser.link/1202010802>

B10. Why would a technician use an ESD strap?

- A. Protect electronic parts from extreme heat
 - B. Keep electronic parts dry and free from moisture
 - C. Prevent damage from static electricity
 - D. Protect computer parts from dust
-

The Answer: C. Prevent damage from static electricity

An ESD (Electrostatic Discharge) strap, or anti-static strap, connects a person to the equipment 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. Protect electronic parts from extreme heat

An ESD strap does not provide any protection for extreme heat or temperature.

B. Keep 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. Protect 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:

220-1202, Objective 4.4 - Managing Electrostatic Discharge

<https://professormesser.link/1202040401>

B11. A technician needs to uninstall a video editing utility from a macOS laptop. Which folder would be the most likely location of this utility?

- A.** /Program Files
 - B.** /Applications
 - C.** /Library
 - D.** /Users
-

The Answer: **B.** /Applications

In macOS, all of the applications are stored in a folder named /Applications. Each application is stored in a separate folder, and most applications can be quickly removed by simply deleting the entire folder.

The incorrect answers:

A. /Program Files

The /Program Files folder is commonly associated with the Windows operating system, and this would not be a location for macOS applications.

C. /Library

The /Library folder contains system files available for multiple users on the macOS system. Shared fonts and system library files would commonly be stored in the /Library folder.

D. /Users

The /Users folder contains most user documents, and this folder name is the same in both Windows and macOS.



More information:

220-1202, Objective 1.8 - macOS Overview

<https://professormesser.link/1202010801>

- B12.** 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 in a project. When the situation is running as expected, a simple update may be the only thing necessary. However, the other participants may want to make alternative plans if problems occur. 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 is the motherboard repair. There will be time after the repair is completed to determine if the shipping process was properly managed.



More information:



220-1202, Objective 4.7 - Communication



<https://professormesser.link/1202040702>

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. diskpart
 - C. robocopy
 - D. dir
-

The Answer: D. dir

The dir (directory) command will display a list of files at 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 which may have been changed since their installation. The sfc command will not display a list of files in the current directory.

B. diskpart

The diskpart command is a command line utility for viewing and managing volumes on a Windows device. The diskpart command does not provide file management.

C. robocopy

The robocopy (Robust Copy) command provides additional features over the copy or xcopy commands. The robocopy utility does not provide the file management features required to search and delete certain files in a directory.



More information:

220-1202, Objective 1.5 - Windows Command Line Tools
<https://professormesser.link/1202010501>

B14. A user runs a corporate app on their smartphone which 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.** Charge the smartphone battery
 - D.** Check the cloud storage resource usage
-

The Answer: **B.** Run a network speed check

Delays associated with the download process would seem to 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 disabling Bluetooth would provide any change to the download speed.

C. Charge the smartphone battery

Although some smartphone features may be limited when battery life is low, it would not cause the delays associated with the current download issue.

D. Check the cloud storage resource usage

The resource usage of a cloud storage platform would not be the most likely cause of the delays with this app.



More information:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

B15. A system administrator is analyzing a problem with a USB flash drive on a Windows 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 device drivers which 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:

220-1202, Objective 1.4

The Microsoft Management Console

<https://professormesser.link/1202010402>

B16. A user is reporting 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 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 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 additional 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:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

B17. A technician has been asked to power down and store a server which 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 to ensure the data on the server is not modified. All access to the data should be tracked, so 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 information to the proper channels doesn't ensure 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:

220-1202, Objective 4.6 - Incident Response

<https://professormesser.link/1202040601>

B18. 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 option which would have resulted in a reinfection if not properly followed. Users aren't malware experts, and they may not realize their actions can have a negative impact 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:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

B19. Which of the following features would be found in Windows 11 Pro but not in Windows 11 Home?

- A. 32-bit and 64-bit versions
 - B. Domain access
 - C. RDP client
 - D. Windows Workgroup
-

The Answer: B. Domain access

Windows 11 Home does not include any access or connectivity to a Windows Domain.

The incorrect answers:

A. 32-bit and 64-bit versions

Windows 11 does not include any 32-bit editions. Windows 11 editions are only available for 64-bit processors.

C. RDP client

An RDP (Remote Desktop Protocol) client is used to connect to an RDP service on another device. All editions of Windows and many non-Windows platforms can use some type of RDP client.

D. Windows Workgroup

A Windows Workgroup is the fundamental networking available in Windows, and it's most often implemented in a home environment. All editions of Windows support connecting to a Windows Workgroup.



More information:

220-1202, Objective 1.3 - Windows Features

<https://professormesser.link/1202010302>

B20. A medical research company is using laptop computers when visiting testing centers. The IT security team is concerned about a 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 application
 - C.** Full disk encryption
 - D.** Biometric authentication
 - E.** Cable lock
-

The Answer: **C.** Full disk encryption

Encrypting the laptop storage drives would prevent access to 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 application

An authenticator application would provide another factor 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 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:

220-1201, Objective 2.2 - Windows Security Settings

<https://professormesser.link/1201020203>

B21. A security administrator is installing a new VPN connection for remote users. The administrator would like all users to authenticate with their Windows Active Directory credentials. Which of the following technologies would provide this functionality?

- A. RADIUS
 - B. WPA3
 - C. TKIP
 - D. AES
-

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. WPA3

WPA3 (Wi-Fi Protected Access version 3) is an 802.11 wireless security protocol. WPA3 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. AES

AES (Advanced Encryption Standard) is an encryption protocol used with many wired and wireless services. AES does not provide authentication features.



More information:

220-1202, Objective 2.3 - Authentication Methods
<https://professormesser.link/1202020302>

B22. A mobile user is using apps on their smartphone for most business tasks. To ensure 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 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:

220-1202, Objective 2.8 - Mobile Device Security
<https://professormesser.link/1202020801>

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 (Solid State Drive) from inadvertent ESD (Electrostatic Discharge) while the component was moved between locations.

The incorrect answers:

A. Padded envelope

A padded envelope would protect against physical damage, 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:

220-1202, Objective 4.4 - Managing Electrostatic Discharge

<https://professormesser.link/1202040401>

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, 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 in 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:

220-1202, Objective 3.4 - Troubleshooting Security Issues

<https://professormesser.link/1202030401>

B25. 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, 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 of the user's home network.

The incorrect answers:

B. Install the latest operating system updates

Since the smartphone works properly in the office, it would be unlikely 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:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices
<https://professormesser.link/1202030201>

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.** Remote network installation
 - 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. Remote network installation

Since this computer has been diagnosed with malware, it would not be a good best practice to reconnect the server to the network.

D. Repair installation

A repair installation is designed to fix problems with the operating system, and it does not commonly 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:

220-1202, Objective 1.2 - Installing Operating Systems
<https://professormesser.link/1202010201>

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 customers can never connect to the company network. Which of the following should be configured on this network?

- A. Install a new access point for company devices
 - B. Configure WPA3 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 WPA3 on the company network

Enabling WPA3 (Wi-Fi Protected Access version 3) would require a password to connect and would prevent customers from connecting to the company wireless network.

The incorrect answers:

A. Install a new access point for company devices

Installing another access point doesn't inherently provide any additional security protections.

C. Require static IP addresses on the customer network

Requiring the configuration of 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:

220-1202, Objective 2.3 - Wireless Encryption

<https://professormesser.link/1202020301>

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 which indicates 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:

220-1202, Objective 3.1 - Troubleshooting Windows
<https://professormesser.link/1202030101>

B29. A company's shipping department maintains ten different computers for printing shipping labels and for tracking outgoing shipments. All of the systems are displaying an error when they 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 are 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 which causes them to fail in exactly the same way would be unusual, so this would not be categorized as the most likely cause of this connectivity issue.



More information:

220-1202, Objective 3.4 - Troubleshooting Security Issues

<https://professormesser.link/1202030401>

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.** Assign an expiration date to the auditor accounts
 - C.** Remove the auditor accounts from all Windows groups
 - D.** Require two-factor authentication for the auditor accounts
-

The Answer: **B.** Assign an expiration date to the auditor accounts

The auditors only need access during certain times of the year, so a good best practice is to create or enable the accounts with a specific expiration date. After this expiration date, the auditors account remains intact but is disabled from the login process.

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 the auditor 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:

220-1202, Objective 2.7 - Security Best Practices

<https://professormesser.link/1202020701>

B31. A manufacturing company is donating some older computers to a local charity. Which of the following should be done to ensure 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, and this would ensure 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 unusable 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:

220-1202, Objective 2.9 - Data Destruction

<https://professormesser.link/1202020901>

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 the building 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:

220-1202, Objective 4.5 - Environmental Impacts

<https://professormesser.link/1202040501>

B33. A desktop administrator is troubleshooting an older computer which 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.** xcopy
 - E.** winver
-

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 which may have changed since their installation.

D. xcopy

The xcopy (Extended Copy) command is used to copy files and directories at the command prompt. The xcopy command does not provide any performance enhancements.

E. winver

The winver (Windows Version) command will display the Windows version dialog on the desktop. The winver command doesn't provide any changes to the operating system performance.



More information:

220-1202, Objective 1.4 - Additional Windows Tools

<https://professormesser.link/1202010403>

B34. A user is receiving alerts on their desktop computer stating, "Access to this PC has been blocked for security reasons." A technician has determined this message was not created by the company's security software. Which of the following would be the best next step in this troubleshooting process?

- A.** Update the desktop computer operating system
 - B.** Check the certificate of the corporate web server
 - C.** Restart the desktop computer
 - D.** Run an anti-malware utility
-

The Answer: **D.** Run an anti-malware utility

A false virus alert could be a static page from a third-party website, but it could also be the result of malware. Performing a malware scan should be the first step in determining the root cause of this issue.

The incorrect answers:

A. Update the desktop computer operating system

Updating the operating system would be a good best practice during this process, but making a change to the OS would not be the best next step.

B. Check the certificate of the corporate web server

There's no error message or notification in this question to indicate an issue with the company's web server.

C. Restart the desktop computer

The troubleshooting process may eventually require the system to be restarted, but it would most likely not be the best next step for this issue. Before restarting, it would be useful to gather as much information as possible.



More information:

220-1202, Objective 3.4 - Troubleshooting Security Issues

<https://professormesser.link/1202030401>

B35. A system administrator has inadvertently installed a Trojan horse which 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 lock
-

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 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 used 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 lock

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:

220-1202, Objective 2.7 - Security Best Practices

<https://professormesser.link/1202020701>

B36. A technician has created a Windows image which can be used across all of the computers in a test lab. Which of the following would be the best way to deploy these images?

- A.** Clean install
 - B.** Remote network installation
 - C.** Repair installation
 - D.** Bootable USB
-

The Answer: **B.** Remote network installation

When installing images to multiple systems, it's more efficient to use the network as a distribution method. This process allows for multiple installations to occur simultaneously without any type of human intervention.

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. A network installation is much more efficient 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. Bootable USB

A bootable USB is a convenient way to transport data, but it doesn't scale easily across multiple systems. To install the image simultaneously to multiple computers, you would need multiple USB keys.



More information:

220-1202, Objective 1.2 - Installing Operating Systems
<https://professormesser.link/1202010201>

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

List folder contents is an NTFS permission configured to allow or deny. These permission categories do not take priority over a deny setting.



More information:

220-1202, Objective 2.2 - Windows Security Settings

<https://professormesser.link/1202020203>

B38. A data center manager would like to ensure any potential 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.** Battery backup
 - C.** Air filter mask
 - D.** ESD mat
-

The Answer: **A.** Electrical ground

An electrical ground will divert 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. Battery backup

A battery backup such as 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 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:

220-1202, Objective 4.4 - Safety Procedures

<https://professormesser.link/1202040402>

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.** Shoulder surfing
-

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 which 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. Shoulder surfing

Shoulder surfing is an attack from someone watching your screen. In this example, the employee in the shipping department does not mention the attacker being in the same room.



More information:

220-1202, Objective 2.5 - Social Engineering

<https://professormesser.link/1202020501>

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 Restore
 - B.** Educate the end-user
 - C.** Quarantine the computer
 - D.** Boot to Safe Mode
-

The Answer: **A.** Enable System Restore

Before the malware was removed, System Restore was disabled to delete all potentially-infected restore points. Once the malware is removed and the anti-malware process is working again, System Restore 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:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

- B41.** A user would like to encrypt a small group of files in a shared folder without modifying other files on the drive. Which of the following would be the best way to accomplish this?
- A.** EFS
 - B.** Save the files with Administrator rights
 - 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 with Administrator rights

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 which 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:

220-1202, Objective 2.2 - Windows Security Settings

<https://professormesser.link/1202020203>

B42. Which of the following partition types limit a Windows installation to a maximum partition size of 2 TB?

- A. FAT32
 - B. GPT
 - C. APFS
 - D. MBR
-

The Answer: D. MBR

The MBR (Master Boot Record) partition style is an older method partitioning files, and the maximum partition size of an MBR partition is two 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 which increases the number of partitions and partition sizes over the older MBR style.

C. APFS

Apple's APFS (Apple File System) is optimized for solid-state storage and includes support for encryption, snapshots, and increased data integrity. APFS would not be used for a Windows installation.



More information:

220-1202, Objective 1.2 - Installing Operating Systems
<https://professormesser.link/1202010201>

B43. A user in the engineering department needs to use some applications written for Windows, but also needs to use applications designed for Linux. Which of the following would be the best way to provide access to these applications?

- A.** Assign the user multiple computers
 - B.** Boot the operating systems from two removable USBs
 - C.** Configure the user's PC for multiboot
 - D.** Compile the Linux applications in Windows
-

The Answer: **C.** Configure the user's PC for multiboot

A computer configured for multiboot will present a list of available operating system options during the startup process. This menu could allow the user to boot Windows or to boot Linux. The user would only need to reboot to switch from one operating system to another.

The incorrect answers:

A. Assign the user multiple computers

Although this would technically solve the issue of multiple operating systems, requiring multiple computers would require additional cost and ongoing management. If the user requires a portable solution, this would introduce additional logistical challenges when mobile.

B. Boot the operating systems from two removable USBs

This solution would also technically work, but it requires the user to maintain (and not lose) the USB keys required to boot and run the system. The performance of the system would also be limited to USB throughput.

D. Compile the Linux applications in Windows

Unfortunately, the code required for a Linux application to work properly in Windows is not seamlessly portable. This Linux code would not compile properly in Windows, so this would not be a viable solution. This would also assume the Linux source code was even available to compile.



More information:

220-1202, Objective 1.2 - Installing Operating Systems

<https://professormesser.link/1202010201>

B44. A help desk technician has been tasked with rebuilding an email server which recently crashed. Which of the following would be the best source for the information required to reconstruct this system?

- 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 could 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. 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 which 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:

220-1202, Objective 4.1 - Document Types

<https://professormesser.link/1202040103>

B45. The employees of a company have direct access to applications and databases from their desktop computers. If the employees are using the company wireless network or the conference room, connectivity is only available after authenticating through a VPN. Which of the following would best describe this policy?

- A. Multifactor authentication
 - B. Group Policy
 - C. Least privilege
 - D. Zero trust
-

The Answer: D. Zero trust

Zero trust is a broad strategy for securing all devices, people, and data within an organization. Zero trust requires verification at every level of access, including the internal wireless networks or network access provided in conference rooms.

The incorrect answers:

A. Multifactor authentication

Multifactor authentication describes the factors provided during the login process, such as a password, security code, or biometric information. Multifactor authentication is not directly part of a policy requiring logins from wireless networks or conference rooms.

B. Group Policy

Group Policy is a management feature associated with Windows Active Directory. Group Policy is not directly associated with the authentication requirements in this question.

C. Least privilege

Least privilege describes the authorization permissions associated with a user account. The goal of least privilege is to only provide rights and permissions matching a user's specific job functions. In this example, the authentication process is not associated with individual user access rights.



More information:

220-1202, Objective 2.1 - Logical Security

<https://professormesser.link/1202020103>

B46. A user has called the help desk to get assistance with random blue screens on their Windows laptop. The technician finds CPU utilization is constantly high, and many network sites are unavailable or only load half of the site content. The user mentions 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 cause network issues or pop-ups.



More information:

220-1202, Objective 3.4 - Troubleshooting Security Issues

<https://professormesser.link/1202030401>

B47. A technician is troubleshooting an issue with an iOS tablet randomly restarting during normal use. A check of the device shows 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 this 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:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

- B48.** A system administrator needs to modify a file in the \Windows\Installer directory, but the folder doesn't appear in the list of available files. 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. Unchecking the option for "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:

220-1202, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1202010601>

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:

220-1202, Objective 1.9 - Linux Commands Part 1

<https://professormesser.link/1202010902>

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 which might also be infected. Once the malware is removed, this feature can be re-enabled.



More information:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

B51. An executive has a laptop which runs very slowly after login and continues running slowly throughout the day. The user has complained certain applications cannot be started and others will randomly crash. A check of the laptop shows 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 cannot commonly be 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 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:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

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.** VPN
 - B.** VNC
 - C.** SSH
 - D.** RDP
-

The Answer: D. RDP

The integrated Windows RDP (Remote Desktop Protocol) feature is used to view and control the screen of a remote computer.

The incorrect answers:

A. VPN

A VPN (Virtual Private Network) is an encrypted tunnel between devices, but the VPN by itself does not provide remote access to the Windows operating system.

B. VNC

VNC (Virtual Network Computing) is a remote desktop application which 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 which can manage the command line of a remote device over an encrypted connection.



More information:

220-1202, Objective 4.9 - Remote Access

<https://professormesser.link/1202040901>

B53. A technician would like to modify a configuration in a user's UEFI BIOS, but the system will not provide a BIOS configuration hotkey after shutting down and powering on the computer. Which of the following would be the best way to address this issue?

- A.** Change the File Explorer Options
 - B.** Modify the Indexing Options
 - C.** Turn off Fast Startup
 - D.** Start the computer in Safe Mode
 - E.** Modify the Ease of Access settings
-

The Answer: **C.** Turn off Fast Startup

Fast Startup can bypass many of the normal startup options, so using the Control Panel Power options for disabling Fast Startup can allow a technician to regain access to the BIOS startup hotkeys.

The incorrect answers:

A. Change the File Explorer Options

There are options in the Control Panel to modify File Explorer options, but none of those options would provide access to the BIOS startup keys.

B. Modify the Indexing Options

The Indexing Options specify which folders should be used during the Windows search process. Modifying the Indexing Options will not allow access to the BIOS startup options.

D. Start the computer in Safe Mode

Starting the computer with Safe Mode would help troubleshoot any ongoing Windows issues, but it would not provide any access to the BIOS configuration.

E. Modify the Ease of Access settings

The Control Panel's Ease of Access settings allow the user to make the computer easier to use, but it doesn't change any of the startup or BIOS configuration options.



More information:

220-1202, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1202010601>

B54. A user has noticed their mouse arrow has been moving around the screen when they are not touching the mouse. The user has watched the mouse opening 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 moving independently and opening 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 this malware infection was part of a recently installed application, it's now likely the malware has infected other parts of the system. Uninstalling the applications would most likely 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:

220-1202, Objective 2.4 - Malware

<https://professormesser.link/1202020401>

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 risk analysis wasn'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 scheduled change to make sure all affected parties have a chance to evaluate the risk and understand the scope of the change. The risk analysis was completed 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 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:

220-1202, Objective 4.2 - Change Management

<https://professormesser.link/1202040201>

B56. A user receives a browser security alert on his laptop when visiting any website which 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:

220-1202, Objective 2.11 - Browser Security

<https://professormesser.link/1202021101>

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 which work in the background
 - F.** Perform a soft reset
-

The Answers: **D.** Disable Bluetooth and cellular connections, and
E. Close apps which work in the background

The two options which would have the largest power savings would disable wireless Bluetooth radios and close applications using extensive CPU power.

The incorrect answers:

A. Install the latest operating system patches

Installing operating system patches do 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 either of these is occurring, so resetting the system would most likely have no effect on the battery life.



More information:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

B58. A system administrator would like to create a Windows distribution which can automatically configure itself to connect to the corporate domain and automatically configure individual user email settings. Which of the following would be the best choice for this requirement?

- A.** Zero-touch deployment
 - B.** Recovery partition installation
 - C.** Image deployment
 - D.** In-place upgrade
-

The Answer: **A.** Zero-touch deployment

A zero-touch deployment allows any user with a customized installation process. This process is a seamless user experience and all domain and account details are automatically configured during the initial installation.

The incorrect answers:

B. Recovery partition installation

A recovery partition can be a good installation option, but it first requires the system be configured with recovery information. The recovery partition would not provide the features required by the system administrator.

C. Image deployment

An image deployment will configure each system exactly the same as every other system. The system administrator would like individual email configurations, so an image deployment would not be the best choice.

D. In-place upgrade

An in-place upgrade will leave user documents and configurations in place during the upgrade process. A new Windows distribution would not have an existing Windows configuration to use as a reference.



More information:

220-1202, Objective 1.2 - Installing Operating Systems

<https://professormesser.link/1202010201>

B59. A user in the accounting department has installed a new application for the upcoming tax year. Although the current application worked perfectly, the newer application runs significantly slower. Which of the following should be the first troubleshooting step?

- A.** Roll back to the previous application
 - B.** Run a repair installation
 - C.** Verify the requirements for the new application
 - D.** Perform a system file check
-

The Answers: **C.** Verify the requirements for the new application

The new application may not have the same requirements as the older application, so the user's computer may require additional CPU power, memory, or storage space.

The incorrect answers:

A. Roll back to the previous application

The previous application may work properly, but it's designed for a different tax year. The new tax year will require an updated application.

B. Run a repair installation

A repair installation can often resolve issues with the Windows operating system, but this question doesn't clearly point to any OS issues. Running a repair installation would not be the first step in the troubleshooting process.

D. Perform a system file check

The Windows System File Checker (SFC) utility can scan the operating system for modified files and correct any inconsistencies. However, this question doesn't clearly show any operating system issues, so running an SFC scan would not be the first step when troubleshooting.



More information:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

B60. A macOS user needs to protect all of the data on their laptop if the laptop is stolen or lost. Which of the following would be the best choice for this requirement?

- A.** Spaces
 - B.** Mission Control
 - C.** FileVault
 - D.** Keychain
-

The Answer: C. FileVault

The FileVault utility provides full disk encryption for macOS devices. If the laptop is lost or stolen, all of the data on the laptop will be encrypted and inaccessible to any third-party.

The incorrect answers:

A. Spaces

Spaces allows a user to configure multiple macOS desktops on the screen. The Spaces feature does not allow the macOS desktop to run Windows applications.

B. Mission Control

Mission Control provides a way to "spread out" the desktop and view all of the running applications on a single desktop screen. Mission Control does not provide any security features or data encryption.

D. Keychain

The macOS Keychain utility maintains and secures passwords, notes, certificates, and other private information. The Keychain does not provide data encryption for user files or documents.



More information:

220-1202, Objective 1.8 - macOS Features

<https://professormesser.link/1202010803>

B61. A data center manager is installing a new access door which will require multi-factor authentication. Which of the following should be used to meet this requirement? (Select TWO)

- A.** Cabinet locks
 - B.** Key fobs
 - C.** Privacy filter
 - D.** Palmprint scanner
 - E.** USB lock
 - F.** Cable lock
-

The Answer: **B.** Key fobs and **D.** Palmprint scanner

The only two devices which provide authentication are the key fobs and the palmprint scanner. The key fobs are something you have, and the palmprint scanner is 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:

220-1202, Objective 2.1 - Physical Access Security

<https://professormesser.link/1202020102>

- B62.** A company is deploying a new set of laptops for field service technicians who travel and work at customer locations. The IT department has been asked to create a secure authentication factor for a minimal cost. Which of the following would be the best choice for this security requirement?
- A.** Retina scanner
 - B.** TOTP app
 - C.** Keyfob
 - D.** Magnetometer
-

The Answer: **B.** TOTP app

A TOTP (Time-based One-Time Password algorithm) app runs on an existing mobile phone or tablet, and the cost is usually quite low compared to physical authentication factors.

The incorrect answers:

A. Retina scanner

A retina scanner is used to view the blood vessels in the back of the eye. The hardware required for this scan would be much more expensive than a mobile app.

C. Keyfob

A keyfob is not as expensive as some of the other options, but there's still a cost associated with purchasing and maintaining physical keyfobs. In this case, the mobile app would be less expensive and easier to manage.

D. Magnetometer

A magnetometer is a device which detects metal, and it's commonly used in the entryway to a building or secure area. A magnetometer would not be used as an authentication factor and the costs would be relatively expensive compared to a mobile app.



More information:

220-1202, Objective 2.1 - Logical Security

<https://professormesser.link/1202020103>

B63. An 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 a malware infection. 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:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

B64. The clock on an executive's Windows laptop has consistently been losing time and is behind by a few minutes at the end of the week. The executive uses this laptop to monitor an assembly line and needs the time and date to be as accurate as possible. Which of these would be the best way to address this issue?

- A. Create a login script to update the date and time
 - B. Configure an NTP server
 - C. Set the clock for a different time zone
 - D. Replace the laptop batteries
-

The Answer: B. Configure an NTP server

A Windows computer can be configured to automatically update the date and time in the Control Panel under Settings > Time & language using NTP (Network Time Protocol).

The incorrect answers:

A. Create a login script to update the date and time

A login script could be used for updating the date and time, but the update would only occur during the login process. For ongoing and integrated clock synchronization, it's best to use the built-in Windows automatic time setting.

C. Set the clock for a different time zone

The issue with this laptop is not related to the time zone, and configuring a different time zone would not prevent the time drift.

D. Replace the laptop batteries

The issue with the time and date is not related to the batteries used to power the laptop. Replacing the batteries would not resolve this time drive issue on the laptop.



More information:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

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 internal data center door? (Select TWO)

- A.** Biometric lock
 - B.** ACL
 - C.** Bollard
 - D.** Additional lighting
 - E.** Motion sensor
 - F.** Access control vestibule
-

The Answer: **A.** Biometric lock and **F.** Access control vestibule

A biometric door lock provides access based on a fingerprint, handprint, or some other biometric characteristic. An access control vestibule is often used to limit or control the flow of people through a particular area. Often an access control vestibule is used in conjunction with additional authentication factors to allow or prevent access to an area.

The incorrect answers:

B. ACL

An ACL (Access Control List) is commonly used by operating systems or other applications to allow or prevent access to a resource. An ACL would not be used to control access to a physical door in a data center.

C. Bollard

A bollard is a barrier which prevents access to a certain area. A bollard would not commonly be used to authenticate users into a data center.

D. Additional lighting

This is an internal door, so it's most likely well lit already. The lights would also not provide any authentication functions for the data center door.

E. Motion sensor

A motion sensor would commonly not be necessary in an open area which receives constant visitors. The motion sensor would not be used in the authentication process.



More information:

220-1202, Objective 2.1 - Physical Security

<https://professormesser.link/1202020101>

- B66.** An administrator is troubleshooting an error message which 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 Monitor to view operational data
 - 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 usually logged in the Event Viewer for review.

The incorrect answers:

A. Use Performance Monitor to view operational data

Performance Monitor provides long-term views of system metrics such as CPU, memory, and network resource usage. Performance Monitor is not used to troubleshoot 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 a determination. Instead of guessing at an issue, it would be more direct and efficient to gather information on the actual error using Windows Event Viewer.



More information:

220-1202, Objective 1.4



The Microsoft Management Console

<https://professormesser.link/1202010402>

B67. Four users in the accounting department have received similar emails asking for payment of an outstanding invoice and a link to a third-party payment site. The emails contains purchase information which appears to be correct, but additional research shows the invoice numbers are not valid. Which of the following would best describe this attack type?

- A. Spear phishing
 - B. Denial of service
 - C. Shoulder surfing
 - D. Evil twin
-

The Answer: A. Spear phishing

A spear phishing attack targets specific individuals or groups, such as accounting department users. These email messages were specific to the accounting team and would not have been applicable to employees in other departments.

The incorrect answers:

B. Denial of service

A denial of service attack uses techniques to disable services or cause extensive outages. This example does not include any system outages.

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. Evil twin

An evil twin is a wireless network which appears to be legitimate but is actually run by the attacker. This issue is not related to connectivity over a wireless network.



More information:

220-1202, Objective 2.5 - Social Engineering

<https://professormesser.link/1202020501>

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" isn't enough information to begin troubleshooting. A quick call to the customer will allow the technician to ask more specific questions and would ultimately 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 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:

220-1202, Objective 4.7 - Communication
<https://professormesser.link/1202040702>

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 and 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 a closed-source mobile operating system for smartphones. iOS is included with the mobile hardware provided by Apple.



More information:

220-1202, Objective 1.1 - Operating Systems Overview

<https://professormesser.link/1202010101>

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 which 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 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:

220-1202, Objective 4.3 - Managing Backups

<https://professormesser.link/1202040301>

B71. A network administrator has a report showing a single user with numerous visits to a website. This website is known to violate 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, the security officer's team should manage the results of this action.

The incorrect answers:

A. Create a firewall filter to block the website

A firewall filter may successfully prevent the user from visiting the site, but the original problem of the user browsing to the site still exists. Creating a firewall filter 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 example which would indicate the inappropriate website was a security risk or 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 which are outside the scope of the AUP violation. This also does not resolve the issue associated with the original website visits.



More information:

220-1202, Objective 4.6 - Privacy, Licensing, and Policies
<https://professormesser.link/1202040602>

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 commonly associated with Microsoft Visual Basic Scripting Edition automation. These scripts provide general purpose scripting in Windows, and are 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 which run at the Windows command line are batch files with the .bat extension. These batch files are not commonly used in Microsoft Office applications.

D. .js

Scripts which 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:

220-1202, Objective 4.8 - Scripting Languages

<https://professormesser.link/1202040801>

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 sharing method for small departments with documents on their own computers.

The incorrect answers:

A. Domain

Microsoft's Active Directory Domain Services are designed for larger organizations which 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:

220-1202, Objective 1.3 - Windows Features

<https://professormesser.link/1202010302>

B74. An employee used their tablet to take pictures of the company's newest product. 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. Cloud storage
 - B. USB flash drive use
 - C. Application updates
 - D. Deleted email messages
-

The Answer: A. Cloud storage

Many mobile devices use cloud storage to backup documents, videos, and photos. Anyone with access to the cloud storage would also have access to all of the photos.

The incorrect answers:

B. USB flash drive use

Using a USB flash drive for storage would not be the most significant security concern, and an attacker would still need to gain physical access to the USB flash drive.

C. Application updates

Applications should always be updated when available, but running older application's wouldn't necessarily provide an attacker with access to the photos.

D. Deleted email messages

There's no mention in this example of any email messages, and deleting messages would not be a security concern.



More information:

220-1202, Objective 3.3

Troubleshooting Mobile Device Security

<https://professormesser.link/1202030301>

- B75.** A manufacturing company in the United States sells monthly subscriptions from their website. Which of the following regulated data types would be the MOST important to manage?
- A. Personal government-issued information
 - B. Credit card transactions
 - C. Healthcare data
 - D. Software license terms
-

The Answer: B. Credit card transactions

The payment card industry has created extensive standards and requirements for accepting and storing credit card transactions.

The incorrect answers:

A. Personal government-issued information

The manufacturing company does not appear to be a governmental organization, so managing government-issued data would not be a significant data management concern.

C. Healthcare data

This example doesn't mention any association with healthcare data, so any regulations around the storage and transmission of healthcare data would not apply.

D. Software license terms

A EULA (End User License Agreement) is commonly associated with software licensing. This example does not mention any license terms, and those terms would usually be publicly available on the website.



More information:

220-1202, Objective 4.6 - Privacy, Licensing, and Policies
<https://professormesser.link/1202040602>

B76. A user is traveling to a conference, and they would like to be sure any messages sent from their phone during the event remain private while using the event's wireless network. 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:

220-1202, Objective 4.9 - Remote Access

<https://professormesser.link/1202040901>

B77. Last week, a computer on the manufacturing floor was upgraded from 8 GB of RAM to 16 GB. Since the upgrade, the system has rebooted itself randomly every few hours. Which of the following would be the best next troubleshooting step?

- A. Run Windows Update
 - B. Perform a hardware diagnostic
 - C. Upgrade the BIOS to the latest version
 - D. Replace the storage drive
-

The Answer: B. Perform a hardware diagnostic

If the only change to the system has been the RAM (Random Access Memory) upgrade, it's likely the problem is something related to this new hardware. Running a hardware diagnostic (and especially a RAM diagnostic) would identify any issues with the new memory modules.

The incorrect answers:

A. Run Windows Update

It's unusual for Windows to reboot every few hours, and it's unlikely a Windows Update patch would resolve an issue which appears to have started with a memory upgrade.

C. Upgrade the BIOS to the latest versions

An outdated BIOS may not have the latest BIOS options available, but it's unlikely to cause random reboots throughout the day. It's always a good best practice to keep your BIOS up to date, but it would not be a useful troubleshooting task for this issue.

D. Replace the storage drive

The storage drive in the computer was not identified as a problem, and replacing the drive is unlikely to solve the rebooting issue. Replacing the drive would also involve the backup and restoration of data, and this would most likely complicate an already difficult issue.



More information:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

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 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 battery backup
 - C.** Create separate file-level backups
 - D.** Perform occasional recovery tests
-

The Answer: **D.** Perform occasional recovery tests

The best way to see if a backup will be useful when needed is to perform occasional audits of the existing backup media. This important step 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 in the backup media.

B. Connect the tape drives to a battery backup

Most of the infrastructure equipment in a data center should be connected to battery backup such as a UPS (Uninterruptible Power Supply), but having a reliable power connection doesn't guarantee 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:

220-1202, Objective 4.3 - Managing Backups

<https://professormesser.link/1202040301>

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 features provides access to these settings?

- A.** Internet Options
 - 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 utility includes configuration options for the browser and configuration settings for proxies.

B. Devices and Printers

The Devices and Printers utility 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:

220-1202, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1202010601>

B80. An Android phone user is traveling internationally and would like to avoid overage charges for using too much cellular data while overseas. Which of the following would be the best way to control data access?

- A. Install a VPN client
 - B. Remove all apps with high data requirements
 - C. Enable data usage notifications
 - D. Connect exclusively through a cellular hotspot
-

The Answer: C. Enable data usage notifications

Android includes the option of notifying the user when a data warning usage value is reached. Android can also block ongoing communication when a specific data limit is met. Many mobile companies will charge based on usage, and this feature helps to limit data overages.

The incorrect answers:

A. Install a VPN client

A VPN client would protect data by encrypting information sent over the network, but a VPN client would not limit or prevent data use after a specific threshold is met.

B. Remove all apps with high data requirements

Removing high-usage apps would be a difficult option to implement, and it ultimately would not prevent other apps from using the network and creating data overages.

D. Connect exclusively through a cellular hotspot

Using a cellular hotspot over 802.11 wireless would certainly limit cellular data usage on the phone, but it simply moves the concern about data overages to the cellular hotspot.



More information:

220-1202, Objective 3.3 -

Troubleshooting Mobile Device Security

<https://professormesser.link/1202030301>

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 inside of a device.

The incorrect answers:

A. Wear safety goggles

Safety goggles aren't commonly required when working inside 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:

220-1202, Objective 4.4 - Safety Procedures

<https://professormesser.link/1202040402>

B82. A system administrator is installing a new video editing application on a user's workstation from a USB flash drive. 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 share 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 share drive for the installation source

Changing the installation media from a USB (Universal Serial Bus) drive to a share 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 modifies 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:

220-1202, Objective 1.10 - Installing Applications

<https://professormesser.link/1202011001>

B83. A user would like to install an image and photo editing program on their home computer, but they would prefer an application without a monthly subscription. Which of the following would be the best licensing option for this requirement?

- A.** Open-source
 - B.** Corporate
 - C.** Personal
 - D.** DRM
-

The Answer: **A.** Open-source

Open-source software is distributed without charge and includes a copy of the source code.

The incorrect answers:

B. Corporate

Software using a corporate 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. DRM

DRM (Digital Rights Management) is a method for managing the licenses used by an organization.



More information:

220-1202, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1202040602>

B84. A system administrator is troubleshooting an application issue. 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:

220-1202, Objective 1.4 - Task Manager

<https://professormesser.link/1202010401>

B85. An administrator is troubleshooting a desktop computer experiencing a reboot issue. 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 failing and resetting during boot.

The incorrect answers:

A. Start Safe Mode and perform a defragmentation

There's no guarantee 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 which are causing the looping to occur.



More information:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

- B86.** A user has downloaded a browser add-on which assists with new car purchases. During the installation, the Windows UAC is requesting permissions to continue with the install. Which of these is most likely?
- 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 which asks for additional permissions when an application wants to make significant changes to the operating system. If a relatively simple application is causing the UAC message to appear, then the application 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 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 the user does not normally have. It's not possible to know what would be downloaded and installed until it actually occurs.



More information:

220-1202, Objective 2.4 - Malware

<https://professormesser.link/1202020401>

B87. A technician is working on many different terminal sessions on their screen from different servers. The technician has also used different authentication credentials on each server. Which of the following would be the best way to display the login name associated with each terminal session?

- A.** winver
 - B.** nslookup
 - C.** whoami
 - D.** net use
-

The Answer: **C.** whoami

The whoami command displays the name of the currently logged-in user. On a system with many different open windows, it's sometimes useful to confirm the username before making changes at the command line.

The incorrect answers:

A. winver

The winver command displays the Windows Version on the current system. The winver command does not provide any information about the current username, however.

B. nslookup

The nslookup (Name Server Lookup) command is used to query information contained on a DNS (Domain Name System) server. The logged in username is not generally part of a DNS server, so the nslookup command would not be the best choice for this task.

D. net use

The net command provides many different Windows-specific features, and using the net use command is commonly associated with mapping a local drive letter to a network share. The net use command does not provide information about the current username.



More information:

220-1202, Objective 1.5 - Windows Command Line Tools
<https://professormesser.link/1202010501>

B88. A system administrator needs a way to deploy new smartphone configurations across four different user groups. Each group will require a different set of email and security configurations. Which of the following would be the best way to setup these smartphones?

- A.** Assign configuration profiles for each group
 - B.** Restore all smartphones from cloud backups
 - C.** Provide customized instructions for each user
 - D.** Assign separate support teams for each group
-

The Answer: **A.** Assign configuration profiles for each group

Most MDMs (Mobile Device Managers) support the use of configuration profiles to simplify the management of multiple groups of mobile devices. A standard set of configuration parameters can be associated with a single group, and this group can then be applied to multiple mobile devices.

The incorrect answers:

B. Restore all smartphones from cloud backups

Since these are new smartphone deployments, there are no cloud backups to restore. These cloud backups would also not provide a way to customize the configurations across different user groups.

C. Provide customized instructions for each user

Although detailed instructions are useful for other IT professionals, it's not effective nor practical to provide the users with detailed instructions for configuring mobile device security settings.

D. Assign separate support teams for each group

Although adding more human capital to this task would effectively solve the issue, this solution would be inefficient, expensive and would not scale with larger and larger user groups. Using automated processes with configuration profiles would be a much more effective solution.



More information:

220-1202, Objective 2.8 - Mobile Device Security
<https://professormesser.link/1202020801>

B89. A desktop administrator is troubleshooting an error which 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:

220-1202, Objective 1.4

The Microsoft Management Console

<https://professormesser.link/1202010402>

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, 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 to 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:

220-1202, Objective 2.10 - Securing a SOHO Network

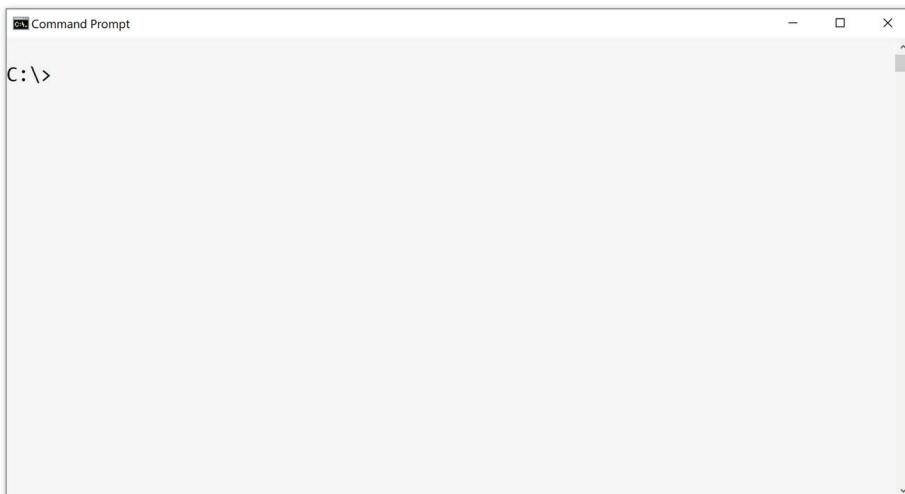
<https://professormesser.link/1202021001>

Practice Exam C

Performance-Based Questions

- C1.** A Windows administrator is troubleshooting a problem with connectivity to a third-party web service at www.professormesser.com. Users are not able to connect to the website and are receiving messages stating the website cannot be reached.

The administrator is concerned their local firewall may be blocking the IP address associated with this website. At the command line, query the default DNS server to determine the IP address of this FQDN.



Answer Page: 299

C2. Choose the best command for the troubleshooting task.

Some commands will not be used.

chmod

fsck

dnf

nano

curl

df

man

grep

A user has requested the installation of a third-party graphics editor

Before installing the third-party graphics editor, the administrator needs to check for available storage space

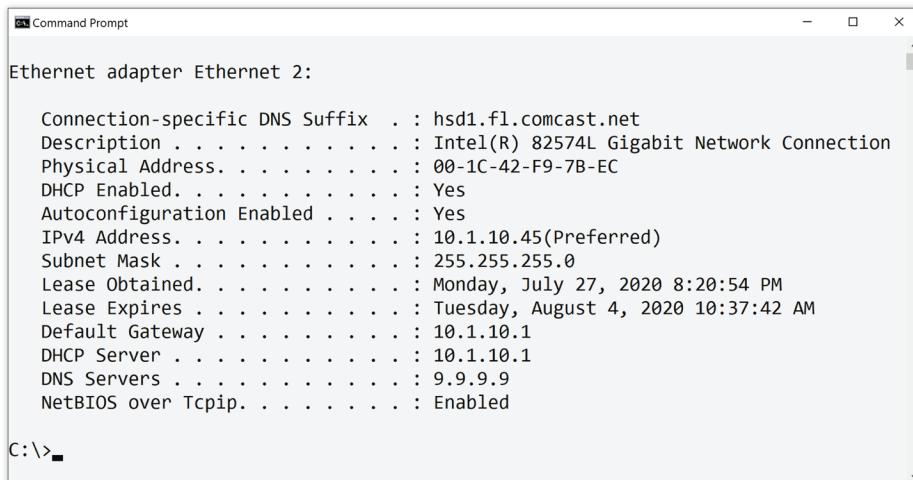
After installing the graphics editor, the administrator makes a minor change to the text-based configuration file

An administrator would like to check the system for orphaned files and file size inconsistencies

A technician needs to find all occurrences of the word "denied" in an authentication log file

Answer Page: 300

- C3.** A user has contacted the help desk because they are not able to browse any websites. The technician suspects a fault with the server which converts fully qualified domain names to IP addresses. What command line would confirm connectivity to this server?



The screenshot shows a Windows Command Prompt window titled "Command Prompt". Inside, the output of the "ipconfig /all" command is displayed for the "Ethernet adapter Ethernet 2:". The configuration details include:

| Setting | Value |
|--------------------------------|--|
| 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 |

At the bottom of the window, the prompt "C:\>—" is visible.

Answer Page: 302

C4. An administrator is configuring the file systems for some new OS installations. Select the best file system for the following:

NTFS

ReFS

ext4

XFS

exFAT

APFS

A user's new Android tablet will be wiped and imaged with the corporate build

A Linux file server is using a large drive array and needs built-in journaling

A department saves files to a USB flash drive and moves the drive between Windows and macOS

A new Windows database server requires large drive support and RAID-like redundancy

A new macOS laptop will be used for mobile video editing and graphics design

A Windows administrator would like to encrypt the data stored in a single shared folder

Answer Page: 303

- C5.** A system administrator is troubleshooting a number of issues with different computers. Pick the administrator's best troubleshooting task for the following issues. Each task will be used once.

Issues:

A desktop computer is running very slowly after login is complete

After starting a laptop, Windows shows the message,
"One or more services failed to start"

A laptop randomly shuts down without any warning or error message

A computer is not able to login due to a certificate trust issue

A user tried to install a Linux distribution on their
Windows computer, but now the system will not boot

A user has received the message,
"The controller does not have enough resources for this device"

Troubleshooting tasks:

 A

Run an overnight series of hardware diagnostics

 B

Connect to a different USB interface

 C

Enable the Windows automatic time setting

 D

Check the authentication credentials in Services

 E

Use Task Manager to view real-time system metrics

 F

Run a Startup Repair or modify the BCD

Answer Page: 304

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: 297
- C7.** A system administrator would like to remove the TFTP Client in Windows. Which of the following Control Panel options would be the best choice for this task?
- A. Programs and Features
 - B. Services
 - C. Network and Sharing Center
 - D. File Explorer options
- The Details: 307
- C8.** A user has noticed a Bluetooth device 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: 297
- The Details: 309

- C9.** A user has recently been assigned a new tablet, but each time she tries to read her email the tablet reboots. The user has reinstalled the email client, but the problem continues to occur. Which of the following would be the best next troubleshooting step?
- A.** Replace the battery
 - B.** Perform a factory reset
 - C.** Run a hardware diagnostic
 - D.** Disable Wi-Fi
- C10.** A computer technician has been asked to verify a set of new Active Directory 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 use
 - B.** sfc
 - C.** gpresult
 - D.** netstat
 - E.** tracert
- 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.** df
 - C.** chown
 - D.** grep

Quick
Answer: **297**

The Details: **310**

Quick
Answer: **297**

The Details: **311**

Quick
Answer: **297**

The Details: **312**

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 option?

- 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: 297

The Details: 313

C13. A home user provides numerous online presentations during the day. However, the power in the area is not stable and there will often be short outages. Which of the following would help with this issue?

- A.** Cloud backups
- B.** External storage device
- C.** Battery backup
- D.** Surge suppressor

Quick
Answer: 297

The Details: 314

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: 297

The Details: 315

C15. A system administrator is concerned about the security of devices in the field and would like to encrypt all data on company laptops. Which of these Windows features would provide this functionality?

- A. EFS
- B. Domain Services
- C. WPA3
- D. BitLocker

Quick
Answer: 297

The Details: 316

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: 297

The Details: 317

C17. A user in the shipping department is authenticating to a third-party package tracking service. After providing a username and password, the site sends an email to the user with a six-digit code to complete the login process. Which of the following would best describe this process?

- A. SPF
- B. ACL
- C. SMS
- D. OTP

Quick
Answer: 297

The Details: 318

C18. A user has opened a help desk ticket with a problem related to email spell checks. A browser-based email client normally checks and corrects the user's grammar and spelling, but the automated checks are no longer working and messages are being sent to customers with grammatical mistakes. Which of the following should the technician check first?

- A.** Proxy settings
- B.** Browser extensions
- C.** Memory utilization
- D.** Web server certificate

Quick
Answer: **297**

The Details: **319**

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: **297**

The Details: **320**

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.** md
- B.** net use
- C.** cd
- D.** dir
- E.** ls

Quick
Answer: **297**

The Details: **321**

C21. A desktop administrator has received a notification of a deployed RSR update. Which of the following would be most affected by this update?

- A.** macOS laptops
- B.** Linux database servers
- C.** Android tablets
- D.** Windows desktops

Quick
Answer: **297**

The Details: **322**

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

Quick
Answer: **297**

The Details: **323**

C23. A Windows computer has one application which crashes randomly throughout the day. Other applications work normally, and the operating system itself runs without any errors. Which of the following would be the best way to address these application crashes?

- A.** Perform a full backup
- B.** Reload the Active Directory profile
- C.** Defragment the hard drive
- D.** Uninstall and reinstall the application

Quick
Answer: **297**

The Details: **324**

C24. An app on a user's corporate smartphone has stopped updating. Which of the following would be the best way to resolve this issue?

- A.** Connect the smartphone to a power source
- B.** Restart the smartphone
- C.** Disable rotation lock
- D.** Disable Bluetooth

Quick
Answer: **297**

The Details: **325**

C25. A technician has been asked to replace a faulty adapter card in a server. The technician doesn't have an anti-static strap, but they have removed the server from the 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: **297**

The Details: **326**

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: **297**

The Details: **327**

C27. A user has started their 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.”

A desktop administrator has confirmed the user can no longer access his desktop, and none of his installed applications are available in the system menus. The user also notices 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.** Ransomware

Quick
Answer: **297**

The Details: **328**

C28. A desktop technician has received a complaint that a remotely-hosted application has stopped working. The technician believes a network outage at the application provider is the root cause of the issue. Which of the following tools would be the best way to confirm the location of the outage?

- A.** ping
- B.** nslookup
- C.** netstat
- D.** tracert

Quick
Answer: **297**

The Details: **329**

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: **297**

The Details: **330**

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: **297**

The Details: **331**

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: **297**

The Details: **332**

C32. The upgrade process for Windows requires the installation of TPM hardware. Which of the following would best describe the reason for this system requirement?

- A.** Wired networking
- B.** 64-bit compatibility
- C.** USB support
- D.** Cryptographic features

Quick
Answer: 297

The Details: 333

C33. A medical center's hospital staff uses shared computer systems installed in hallways and patient rooms. However, hospital administrators are concerned 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: 297

The Details: 334

C34. A user has a smartphone to assist with maps and directions when traveling to other company locations. At a remote site, the user finds his phone 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: 297

The Details: 335

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.** AES
- B.** TKIP
- C.** RADIUS
- D.** WPA3

Quick
Answer: 297

The Details: 336

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 now shows a Stop Error and reboots 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: 297

The Details: 337

C37. A security administrator is deploying a new application to users in the field, but the administrator is concerned simply using a username and password does not provide enough security. Which of the following would be the best way to address this issue?

- A.** Enable Windows Firewall
- B.** Block all login attempts at the Internet firewall
- C.** Create a Group Policy
- D.** Require multi-factor authentication
- E.** Enable BitLocker on all remote systems

Quick
Answer: 297

The Details: 338

C38. A system administrator would like to upgrade a user's Windows video editing application to the latest version, but the upgrade utility fails with the error "Not enough free space." Which of the following utilities would allow the system administrator to resolve this issue?

- A.** cleanmgr
- B.** perfmon
- C.** eventvwr
- D.** taskschd
- E.** diskmgmt

Quick
Answer: **297**

The Details: **339**

C39. A user in the shipping department is using a tracking app on a tablet. The app normally takes 10 seconds to load, but now takes over a minute before it can be used. Tracking searches which 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 reboot

Quick
Answer: **297**

The Details: **340**

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: **297**

The Details: **341**

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: **297**

The Details: **342**

C42. A Windows administrator needs to define a minimum password length for all network users. Which of the following should be used to complete this task?

- A. Device Manager
- B. Certificate Manager
- C. Group Policy Editor
- D. Performance Monitor

Quick
Answer: **297**

The Details: **343**

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. Organizational Units

Quick
Answer: **297**

The Details: **344**

C44. A user is receiving this message on their Windows desktop: "The controller does not have enough resources for this device." Which of the following would be the most likely reason for this issue?

- A. Remote printer has been disabled
- B. Wireless network bandwidth exceeded
- C. USB endpoints are exceeded
- D. The system clock is incorrect

Quick
Answer: **297**

The Details: **345**

C45. A small company is located in a large office building shared by 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.** WPA3 encryption
- D.** SSID suppression

Quick
Answer: **297**

The Details: **346**

C46. A manager in the accounting department would like to upgrade to Windows 11, 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.** Image deployment
- C.** Remote network installation
- D.** In-place upgrade

Quick
Answer: **297**

The Details: **347**

C47. A network administrator has modified all wireless access points to use WPA3 instead of WPA2. Which of the following would be a reason for this change?

- A.** Additional frequency choices
- B.** Lower power consumption
- C.** Larger usable range
- D.** Stronger encryption

Quick
Answer: **297**

The Details: **348**

C48. A help desk is receiving reports associated with a group of devices 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. Metered connection

Quick
Answer: 297

The Details: 349

C49. A user created some documents on their laptop SSD yesterday, but today has reported a problem accessing the files. They are receiving the message, "You require permission to make changes to this file." Which of the following would be the best next troubleshooting step?

- A. Scan for malware
- B. Change the boot drive in the BIOS
- C. Restart the operating system
- D. Defragment the drive

Quick
Answer: 297

The Details: 350

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: 297

The Details: 351

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: 297

The Details: 352

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.** Secure wireless communication
- C.** Encrypted network tunnel
- D.** Full disk encryption

Quick
Answer: 297

The Details: 353

C53. A technician has been tasked with updating the BIOS of any Windows device using an older BIOS version. The technician cannot reboot these systems to check the BIOS versions currently in use. Which of the following would be the best way to proceed?

- A.** Install the BIOS upgrade regardless of the version
- B.** View BIOS information in Group Policy Editor
- C.** Run a report using Performance Monitor
- D.** Use System Information to view the BIOS version

Quick
Answer: 297

The Details: 354

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 which 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: 297

The Details: 355

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.** Battery backup
- B.** Cloud storage
- C.** RADIUS administration servers
- D.** Image-level backups

Quick
Answer: 297

The Details: 356

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 the shared folders are no longer in the list of available storage drives. The user confirms 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: 297

The Details: 357

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.** Corporate license
- C.** Open-source license
- D.** End user licensing agreement

Quick
Answer: 297

The Details: 358

C58. A client's desktop computer is randomly rebooting throughout the workday without any warnings or error messages. Which of the following would be the best next troubleshooting step?

- A.** Update the system BIOS
- B.** Reinstall the Windows operating system
- C.** Boot to Safe Mode and disable all startup applications
- D.** Perform a full system diagnostic

Quick
Answer: **297**

The Details: **359**

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: **297**

The Details: **360**

C60. A laptop in the accounting department has been infected with malware, and the technician has just completed the removal process. Which of the following would be the best way to verify the integrity of the core operating system files?

- A.** Perform a clean Windows install
- B.** Run the system file check utility
- C.** Rebuild the Windows profile
- D.** Roll back the last Windows update

Quick
Answer: **297**

The Details: **361**

C61. A user has noticed 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: 297

The Details: 362

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 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: 297

The Details: 364

C63. A user's smartphone contains company confidential information which 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. Locator application
- B. Remote wipe
- C. Authenticator app
- D. Cloud backup

Quick
Answer: 297

The Details: 365

C64. A user would like to configure their local printer to be accessible to anyone on the corporate network. Which of the following would be the best way to configure this connection?

- A.** Configure a VPN connection
- B.** Create a share name in printer properties
- C.** Configure a metered connection
- D.** Use a static IP address

Quick
Answer: **297**

The Details: **366**

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: **297**

The Details: **367**

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.** APFS
- C.** NTFS
- D.** ext4

Quick
Answer: **297**

The Details: **368**

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 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.** Restart the computer
- B.** Perform a Startup Repair
- C.** Start in VGA mode
- D.** Rebuild the user's profile

Quick
Answer: **297**

The Details: **369**

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: **297**

The Details: **370**

C69. A workstation technician manages a training center with 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: **297**

The Details: **371**

C70. A user would like to use their smartphone for a payment during checkout at the grocery store, but the smartphone is not seen by the payment system. Which of the following would be the BEST next troubleshooting step?

- A.** Restart the smartphone
- B.** Replace the battery
- C.** Perform a factory reset
- D.** Enable Wi-Fi

Quick
Answer: **297**

The Details: **372**

C71. A technician is troubleshooting a problem with user's laptop and very high utilization, even with no activity on the screen or user input to the operating system. Task Manager shows 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 DDoS attack
- D.** Network adapter is faulty

Quick
Answer: 297

The Details: 373

C72. A user's smartphone app shows a splash screen but disappears after a few seconds. Which of the following would be the best way for a technician to view logs and memory statistics for the app?

- A.** Developer mode
- B.** Cloud storage
- C.** Jailbreaking
- D.** Application spoofing

Quick
Answer: 297

The Details: 374

C73. A company has created an internal process to ensure 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: 297

The Details: 375

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 guest account
- E.** Enable file storage quotas
- F.** Enable password complexity

Quick
Answer: **297**

The Details: **376**

C75. A user has purchased a computer which 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: **297**

The Details: **377**

C76. A financial services company is upgrading the storage drives in their SAN and need to dispose of one hundred older storage drives. The security administrator would like to permanently disable the drive and guarantee the data on the drives 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: **297**

The Details: **378**

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: 297

The Details: 379

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.** Standard operating procedures
- D.** Regulatory compliance documentation

Quick
Answer: 297

The Details: 380

C79. A healthcare administrator stores sensitive data on his laptop computer. His desk is in an open area near a busy hallway. Which of the following would add additional security to the administrator's work area?

- A.** Door lock
- B.** Fingerprint scanner
- C.** Magnetometer
- D.** Bollards

Quick
Answer: 297

The Details: 381

C80. A technician has received a help desk ticket asking for help with a broken laptop keyboard. After calling the user, the technician learns the laptop is scheduled to be used for a press event the following day. Which of the following would be the best next step with the ticket?

- A.** Refer the ticket to the laptop group
- B.** Escalate the issue with management
- C.** Add the event information to the problem description
- D.** Assign the ticket to the "laptop" category

Quick
Answer: 297

The Details: 382

C81. A network administrator has been asked to manage the router configurations at all company locations. Which of the following would be the best choice for this task?

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

Quick
Answer: **297**

The Details: **383**

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

Quick
Answer: **297**

The Details: **384**

C83. A technician has just received fifty boxes of used laser printer toner cartridges 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.** Incinerate the cartridges
- D.** Drill a hole in each cartridge

Quick
Answer: **297**

The Details: **385**

C84. A system administrator has been notified 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 for the change control 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: **297**

The Details: **386**

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: **297**

The Details: **387**

C86. A technician is troubleshooting a problem on a Linux server and needs to view the real-time CPU and memory utilization for each operating system process. Which of the following would provide this functionality?

- A.** dig
- B.** df
- C.** cat
- D.** top

Quick
Answer: **297**

The Details: **388**

C87. A technician has just installed a new device driver and restarted a Windows laptop, but now the system shows a Windows Stop Error before the login screen is displayed. Which of the following would be the best way to resolve this issue?

- A.** Start in Safe Mode
- B.** Replace the system memory
- C.** Reinstall Windows from the original media
- D.** Perform a full backup

Quick
Answer: 297

The Details: 389

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: 297

The Details: 390

C89. A company has configured a server for daily backups, and a full backup is created each Sunday based on the previous incremental backups. Which of the following would best describe this backup strategy?

- A.** Differential
- B.** GFS
- C.** Synthetic
- D.** 3-2-1

Quick
Answer: 297

The Details: 391

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: 297

The Details: 392

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

Performance-Based Answers

- C1. A Windows administrator is troubleshooting a problem with connectivity to a third-party web service at www.professormesser.com. Users are not able to connect to the website and are receiving messages stating the website cannot be reached.

The administrator is concerned their local firewall may be blocking the IP address associated with this website. At the command line, query the default DNS server to determine the IP address of this FQDN.



```
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 query a DNS server for information about IP addresses, fully qualified domain names, email server addresses, and other important name services.

In this example, the command "nslookup www.professormesser.com" provides three separate IP addresses, and any of those IP addresses can be used by the local computer to connect to the www.professormesser.com website.



More information:

220-1202, Section 1.5 - The Windows Network Command Line
<https://professormesser.link/1202010502>

C2. Choose the best command for the troubleshooting task.

Some commands will not be used.

dnf

A user has requested the installation of a third-party graphics editor

The dnf (Dandified YUM) utility is a package manager for Linux, and it's primarily used to install and update software in the operating system.

df

Before installing the third-party graphics editor, the administrator needs to check for available storage space

The df (Disk Free) command shows the file systems in use and how much free space is available.

nano

After installing the graphics editor, the administrator makes a minor change to the text-based configuration file

Nano is a full-screen text editor for Linux, and it's included with most Linux distributions and installations.

fsck

An administrator would like to check the system for orphaned files and file size inconsistencies

The fsck (File System Check) utility will check the file system and resolve any file size inconsistencies, orphaned files, or any other logical file system errors.

grep

A technician needs to find all occurrences of the word "denied" in an authentication log file

The grep command is used to find text in a file. This utility can quickly find a specific string in very large text files.

Commands not used:

chmod:

The chmod (Change Mode) command allows the user to change the access (mode) of a file to read, write, execute, or a combination of those permissions.

curl:

The curl (Client URL) utility retrieves web page and displays the raw HTML data associated with the page content. Once retrieved, this data can be easily searched or parsed by a script or other form of automation.

man:

The man (Manual) utility provides command line access to the documentation of other Linux features.



More information:

220-1202, Section 1.9- Linux Commands Part 1

<https://professormesser.link/1202010901>



More information:

220-1202, Section 1.9- Linux Commands Part 2

<https://professormesser.link/1202010902>

- C3.** A user has contacted the help desk because they are not able to browse any websites. The technician suspects a fault with the server which converts fully qualified domain names to IP addresses. What command line would confirm connectivity to this server?

```
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 which 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 to the device.



More information:

220-1202, Objective 1.5

The Windows Network Command Line

<https://professormesser.link/1202010502>

C4. An administrator is configuring the file systems for some new OS installations. Select the best file system for the following:

A user's new Android tablet will be wiped and imaged with the corporate build

ext4

The ext4 file system (Fourth extended file system) is commonly associated with Linux and the Android operating systems.

A Linux file server is using a large drive array and needs built-in journaling

XFS

XFS (Extended File System) is a high-performance file system for Linux.

A department saves files to a USB flash drive and moves the drive between Windows and macOS

exFAT

exFAT (Extended File Allocation Table) is a Microsoft file system designed for USB flash drives and similar removable flash storage.

A new Windows database server requires large drive support and RAID-like redundancy

ReFS

ReFS (Resilient File System) is designed to be the future of Windows file systems, and it's common to see ReFS used on newer high-performance application servers.

A new macOS laptop will be used for mobile video editing and graphics design

APFS

The APFS (Apple File System) is optimized for solid-state storage devices and include support for encryption, snapshots, and increased data integrity.

A Windows administrator would like to encrypt the data stored in a single shared folder

NTFS

The Windows operating system runs optimally using the NTFS (NT File System), and most Windows devices will be configured with NTFS by default.



More information:

220-1202, Section 1.1 - File Systems

<https://professormesser.link/1202010102>

C5. A system administrator is troubleshooting a number of issues with different computers. Pick the administrator's best troubleshooting task for the following issues. Each task will be used once.



A desktop computer is running very slowly after login is complete



E Use Task Manager to view real-time system metrics

When a system is exhibiting poor performance, it can be difficult to determine which part of the system may be causing the issue. Task Manager provides independent view of performance for CPU, memory, disk access, network communication, and more.



After starting a laptop, Windows shows the message,
"One or more services failed to start"



D Check the authentication credentials in Services

All of the Windows background services are managed in the Services app, and some of the services require additional authentication credentials to properly start. The "Log On" tab for an individual service contains the option to log on as a local System account or with a specific username and password.



A laptop randomly shuts down without any warning or error message



A Run an overnight series of hardware diagnostics

When a problem with a system occurs, error messages are normally displayed on the screen. If a system is randomly powering down or restarting, the issue may be related to a hardware issue. Running hardware diagnostics overnight can provide extensive testing of each individual hardware component and hopefully determine which piece of hardware may be causing this random shutdown issue.

A computer is not able to login due to a certificate trust issue

C Enable the Windows automatic time setting

Cryptographic processes often require time synchronization between devices. If the time and date between devices is different by more than a few minutes, the cryptographic functions for authentication or web site encryption may not work properly.

A user tried to install a Linux distribution on their Windows computer, but now the system will not boot

F Run a Startup Repair or modify the BCD

The BCD (Boot Configuration Data) contains the information needed to properly locate and start the Windows operating system. If the boot manager or the BCD are modified, the system will not be able to locate Windows during the boot process.

A user has received the message,
"The controller does not have enough resources for this device"

B Connect to a different USB interface

USB devices contain buffers called "endpoints." If all of the endpoints are used on a USB controller, this error message will appear. Moving the device to a different USB interface managed by a different USB controller will usually allow the USB device to access the required number of endpoints.



More information:

220-1202, Section 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

Practice Exam C

Multiple Choice Detailed Answers

- 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:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

C7. A system administrator would like to remove the TFTP Client in Windows. Which of the following Control Panel options would be the best choice for this task?

- A.** Programs and Features
 - B.** Services
 - C.** Network and Sharing Center
 - D.** File Explorer options
-

The Answer: **A.** Programs and Features

The Programs and Features option 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. Network and Sharing Center

The Network and Sharing Center manages all network adapters and sharing settings in Windows. The Network and Sharing Center does not enable or disable individual application use.

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:

220-1202, Objective 1.6 - The Windows Control Panel

<https://professormesser.link/1202010601>

C8. A user has noticed a Bluetooth device 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 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 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:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices
<https://professormesser.link/1202030201>

C9. A user has recently been assigned a new tablet, but each time she tries to read her email the tablet reboots. The user has reinstalled the email client, but the problem continues to occur. Which of the following would be the best next troubleshooting step?

- A. Replace the battery
 - B. Perform a factory reset
 - C. Run a hardware diagnostic
 - D. Disable Wi-Fi
-

The Answer: C. Run a hardware diagnostic

A new tablet would not commonly exhibit random reboots, so checking the hardware would be a good first step.

The incorrect answers:

A. Replace the battery

The tablet battery did not appear to be an issue, and it would be unusual for a new tablet to have a faulty battery. The system is also rebooting, so the tablet would restart back to the initial screen. This would not indicate an issue with the battery.

B. Perform a factory reset

A factory reset would delete everything on the tablet, and it's not a good best practice to start the troubleshooting process by deleting all user data.

D. Disable Wi-Fi

An active Wi-Fi adapter would not generally cause a tablet to reset, so disabling the Wi-Fi connection would most likely not have any use during the troubleshooting process.



More information:

220-1202, Objective 3.4 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030401>

C10. A computer technician has been asked to verify a set of new Active Directory 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 use
 - B.** sfc
 - C.** gpresult
 - D.** netstat
 - E.** tracert
-

The Answer: **C.** gpresult

The gpresult (Group Policy Results) utility will display the Active Directory policy settings associated with a computer or user.

The incorrect answers:

A. net use

The net use command assigns a drive letter to a network share. The net use command will not display Group Policy information.

B. sfc

The sfc (System File Checker) command will scan the integrity of all protected system files and repair any which 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. tracert

The tracert (traceroute) command can be used to build a list of routes between IP subnets.



More information:

220-1202, Objective 1.5 - Windows Command Line Tools

<https://professormesser.link/1202010501>

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.** df
 - 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. df

The df (Disk Free) command displays the Linux file systems and the available and used space on each file system.

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:

220-1202, Objective 1.9 - Linux Commands Part 1

<https://professormesser.link/1202010902>

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 option?

- 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 some options for traveling 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 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:

220-1202, Objective 4.7 - Communication

<https://professormesser.link/1202040702>

C13. A home user provides numerous online presentations during the day. However, the power in the area is not stable and there will often be short outages. Which of the following would help with this issue?

- A.** Cloud backups
 - B.** External storage device
 - C.** Battery backup
 - D.** Surge suppressor
-

The Answer: **C.** Battery backup

A battery backup can provide ongoing backup power when 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:

220-1202, Objective 4.5 - Environmental Impacts

<https://professormesser.link/1202040501>

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 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:

220-1202, Objective 4.2 - Change Management

<https://professormesser.link/1202040201>

C15. A system administrator is concerned about the security of devices in the field and would like to encrypt all data on company laptops. Which of these Windows features would provide this functionality?

- A.** EFS
 - B.** Domain Services
 - C.** WPA3
 - D.** BitLocker
-

The Answer: D. BitLocker

BitLocker is a Windows feature providing full disk encryption of entire volumes. All data stored on a laptop using BitLocker is encrypted by default.

The incorrect answers:

A. EFS

EFS (Encrypting File System) encrypts file system objects on a Windows computer. EFS does not generally provide encryption of all files on a storage drive or volume.

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. WPA3

WPA3 is a wireless security protocol and does not provide any security for data stored on a laptop.



More information:

220-1202, Objective 1.3 - Windows Features

<https://professormesser.link/1202010302>

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 to 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 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:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

C17. A user in the shipping department is authenticating to a third-party package tracking service. After providing a username and password, the site sends an email to the user with a six-digit code to complete the login process. Which of the following would best describe this process?

- A. SPF
 - B. ACL
 - C. SMS
 - D. OTP
-

The Answer: D. OTP

An OTP (One-Time Password) is used to provide an additional authentication factor during the login process. These one-time passwords will commonly be provided through some type of personal communication method, such as email or text-message.

The incorrect answers:

A. SPF

SPF (Sender Policy Framework) is an email verification process used between email servers to verify the authorized email servers for a specific domain. SPF is not used for individual user authentication factors.

B. ACL

An ACL (Access Control List) is used by an operating system or application process to determine if a specific process, traffic flow, or function is allowed to proceed. An email containing an authentication factor is not an ACL.

C. SMS

SMS (Short Message Service) is also known as text messaging, and it's commonly used as an authentication factor of something you have. In this example, the login code was provided using email and not by text message.



More information:

220-1202, Objective 2.1 - Logical Security
<https://professormesser.link/1202020103>

C18. A user has opened a help desk ticket with a problem related to email spell checks. A browser-based email client normally checks and corrects the user's grammar and spelling, but the automated checks are no longer working and messages are being sent to customers with grammatical mistakes. Which of the following should the technician check first?

- A.** Proxy settings
 - B.** Browser extensions
 - C.** Memory utilization
 - D.** Web server certificate
-

The Answer: **B.** Browser extensions

Browser extensions are used to add new features into an existing browser. Many browser-based spell check and grammar features require the installation of a browser extension to enable this functionality.

The incorrect answers:

A. Proxy settings

Proxies are often used as a connection between the internal network and Internet websites. If the proxy information was incorrect, there would most likely be other issues with loading or accessing third-party websites.

C. Memory utilization

Applications will certainly have issues when available RAM (Random Access Memory) is low, but those issues usually include detailed error messages and information regarding available memory. In this example, there's no mention of error messages or memory problems.

D. Web server certificate

The web server certification provides website verification and encryption functionality, but the certificate on the web server is not usually associated with webpage content issues.



More information:

220-1202, Objective 2.11 - Browser Security
<https://professormesser.link/1202021101>

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 which 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:

220-1202, Objective 2.5 - Password Attacks

<https://professormesser.link/1202020505>

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.** md
 - B.** net use
 - C.** cd
 - D.** dir
 - E.** ls
-

The Answer: **A.** md

The md (Make Directory) command is used to create a subdirectory or folder on the file system.

The incorrect answers:

B. net use

The net command is used for many different Windows-related functions. 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:

220-1202, Objective 1.5 - Windows Command Line Tools

<https://professormesser.link/1202010501>

C21. A desktop administrator has received a notification of a deployed RSR update. Which of the following would be most affected by this update?

- A.** macOS laptops
 - B.** Linux database servers
 - C.** Android tablets
 - D.** Windows desktops
-

The Answer: **A.** macOS laptops

A macOS system can be configured to receive RSR (Rapid Security Response) updates. These RSR updates will push patches to all macOS, iOS, and iPadOS systems automatically when critical security changes or zero-day updates are required.

The incorrect answers:

B. Linux database servers

A Linux database server is not part of an RSR update process. Linux includes many different update and patching features within its own operating system.

C. Android tablets

Android tablet updates are pushed out as needed, but these updates are not part of the Apple Rapid Security Response process.

D. Windows desktops

Windows desktops use Windows Update to push out application patches, operating system changes, and security updates.



More information:

220-1202, Objective 1.8 - macOS Overview

<https://professormesser.link/1202010801>

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:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

C23. A Windows computer has one application which crashes randomly throughout the day. Other applications work normally, and the operating system itself runs without any errors. Which of the following would be the best way to address these application crashes?

- A. Perform a full backup
 - B. Reload the Active Directory profile
 - C. Defragment the hard drive
 - D. Uninstall and reinstall the application
-

The Answer: D. Uninstall and reinstall the application

Once an application is installed, it's important to avoid overwriting any of the application files or libraries. Maintaining the state of configuration files and registry entries are also important, since any changes can create application instability. Uninstalling the application and installing a fresh version can often resolve these stability issues.

The incorrect answers:

A. Perform a full backup

It's always good to have a backup, but this issue appears to be related to a single application. In this case, having a backup is not going to address the root problem of the application crashes.

B. Reload the Active Directory profile

Active Directory profiles are stored on the central AD servers, and the profiles are downloaded to a system during the login process. Although these profiles can sometimes have problems or delays during the download process, this would not usually cause a single application to fail.

C. Defragment the hard drive

The constant reading and writing of data can be made more efficient by running a hard drive defragmentation, but this defrag process would not resolve any issues associated with application instability.



More information:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

C24. An app on a user's corporate smartphone has stopped updating. Which of the following would be the best way to resolve this issue?

- A. Connect the smartphone to a power source
 - B. Restart the smartphone
 - C. Disable rotation lock
 - D. Disable Bluetooth
-

The Answer: B. Restart the smartphone

The update process for the app may need to be restarted, and the easiest way to reinitialize the process is to restart the smartphone.

The incorrect answers:

A. Connect the smartphone to a power source

Providing a power source would not commonly initialize any download services.

C. Disable rotation lock

The rotation lock on a smartphone prevents it from automatically transitioning between portrait and landscape orientations. Modifying the lock status would not provide any assistance with app updates.

D. Power off all Bluetooth devices

It would be unusual for Bluetooth devices to cause problems with the app update process. Powering off Bluetooth devices would not enable the app update process.



More information:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

C25. A technician has been asked to replace a faulty adapter card in a server. The technician doesn't have an anti-static strap, but they have removed the server from the 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 a 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:

220-1202, Objective 4.4 - Managing Electrostatic Discharge

<https://professormesser.link/1202040401>

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 for the Windows operating system. PowerShell provides integrations 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 website's user interface. 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:

220-1202, Objective 4.8 - Scripting Languages

<https://professormesser.link/1202040801>

C27. A user has started their 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.”

A desktop administrator has confirmed the user can no longer access his desktop, and none of his installed applications are available in the system menus. The user also notices 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.** Ransomware
-

The Answer: D. Ransomware

Ransomware is malware which encrypts data files and requires payment before the files can be decrypted.

The incorrect answers:

A. Spyware

Spyware 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 which 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:

220-1202, Objective 2.4 - Malware

<https://professormesser.link/1202020401>

C28. A desktop technician has received a complaint that a remotely-hosted application has stopped working. The technician believes a network outage at the application provider is the root cause of the issue. Which of the following tools would be the best way to confirm the location of the outage?

- A.** ping
 - B.** nslookup
 - C.** netstat
 - D.** tracert
-

The Answer: **D.** tracert

The tracert (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 identify devices on the network, 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:

220-1202, Objective 1.5 -

The Windows Network Command Line

<https://professormesser.link/1202010502>

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 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 providing 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:

220-1202, Objective 2.1 - Authentication and Access

<https://professormesser.link/1202020104>

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:

220-1202, Objective 4.4 - Managing Electrostatic Discharge
<https://professormesser.link/1202040401>

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 a specific text string.

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:

220-1202, Objective 1.9 - Linux Commands Part 1

<https://professormesser.link/1202010902>

- C32.** The upgrade process for Windows requires the installation of TPM hardware. Which of the following would best describe the reason for this system requirement?
- A. Wired networking
 - B. 64-bit compatibility
 - C. USB support
 - D. Cryptographic features
-

The Answer: D. Cryptographic features

A TPM (Trusted Platform Module) is a hardware feature on the motherboard which supports security features such as BitLocker, Windows Hello, and other cryptographic functions. Full Windows 11 support requires the installation of hardware supporting TPM version 2.0.

The incorrect answers:

A. Wired networking

A TPM is not associated with networking or wired Ethernet connectivity. A network connection in Windows works optimally without a TPM.

B. 64-bit compatibility

The operating system determines compatibility with 32-bit or 64-bit software, and a 64-bit operating system is required to support 64-bit applications. A TPM does not determine the support for 32-bit or 64-bit applications.

C. USB support

USB (Universal Serial Bus) connections do not require a TPM.



More information:

220-1202, Objective 1.2 - Upgrading Windows

<https://professormesser.link/1202010202>

C33. A medical center's hospital staff uses shared computer systems installed in hallways and patient rooms. However, hospital administrators are concerned 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 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 to 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 which 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:

220-1202, Objective 2.7 - Security Best Practices
<https://professormesser.link/1202020701>

C34. A user has a smartphone to assist with maps and directions when traveling to other company locations. At a remote site, the user finds his phone 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 (Global Positioning System) 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, 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:

220-1202, Objective 3.3

Troubleshooting Mobile Device Security

<https://professormesser.link/1202030301>

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. AES
 - B. TKIP
 - C. RADIUS
 - D. WPA3
-

The Answer: C. RADIUS

RADIUS (Remote Authentication Dial-in User Service) is an authentication protocol used to integrate with many existing 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. AES

AES (Advanced Encryption Standard) is an encryption protocol, and AES is not used to 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. WPA3

WPA3 (Wi-Fi Protected Access version 3) is an encryption technology for 802.11 wireless networks. WPA3 does not provide authentication integration to Active Directory databases.



More information:

220-1202, Objective 2.3 - Authentication Methods
<https://professormesser.link/1202020302>

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 now shows a Stop Error and reboots 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 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 modifications, 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:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

C37. A security administrator is deploying a new application to users in the field, but the administrator is concerned simply using a username and password does not provide enough security. Which of the following would be the best way to address this issue?

- A.** Enable Windows Firewall
 - B.** Block all login attempts at the Internet firewall
 - C.** Create a Group Policy
 - D.** Require multi-factor authentication
 - E.** Enable BitLocker on all remote systems
-

The Answer: **D.** Require multi-factor authentication

Multi-factor authentication requires additional login credentials, and this process should provide the security required for remote device logins.

The incorrect answers:

A. Enable Windows Firewall

Windows Firewall does not include a method for enhancing the security of an application's login process.

B. Block all login attempts at the Internet firewall

The users in the field are authenticating to the application. Blocking those login attempts would effectively disable the application.

C. Create a Group Policy

Using Windows Group Policy can manage the use of the operating system, but it would not modify the security for a third-party application.

E. Enable BitLocker on all remote systems

Using BitLocker would encrypt all data on the storage drive of a laptop, but it would not provide enhanced authentication for a third-party application or system.



More information:

220-1202, Objective 2.1 - Logical Security

<https://professormesser.link/1202020103>

C38. A system administrator would like to upgrade a user's Windows video editing application to the latest version, but the upgrade utility fails with the error "Not enough free space." Which of the following utilities would allow the system administrator to resolve this issue?

- A.** cleanmgr
 - B.** perfmon
 - C.** eventvwr
 - D.** taskschd
 - E.** diskmgmt
-

The Answer: **A.** cleanmgr

The cleanmgr.exe (Disk Cleanup) utility will find unused or unneeded files and remove them from the file system. This might include temporary Internet files, error reports, downloaded program files, and others.

The incorrect answers:

B. perfmon

The perfmon.msc (Performance Monitor) utility displays long-term graphs and collects data regarding CPU, network, memory, and other system resources.

C. eventvwr

The eventvwr.msc (Event Viewer) utility provides a log of all operating system, application, and security events in Microsoft Windows.

D. taskschd

The Windows taskschd.msc (Task Scheduler) allow the scheduling of an application or script.

E. diskmgmt

Disk operations can be managed through the diskmgmt.msc (Disk Management) utility.



More information:

220-1202, Objective 1.4 - Additional Windows Tools

<https://professormesser.link/1202010403>

C39. A user in the shipping department is using a tracking app on a tablet.

The app normally takes 10 seconds to load, but now takes over a minute before it can be used. Tracking searches which 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 reboot
-

The Answer: D. Perform a reboot

Before making any significant changes, a reboot should 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 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:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

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 with carbon dioxide, FM-200, or other dry chemicals would be the best choice for electronic equipment.

The incorrect answers:

A. Foam

A 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 which can be used safely while putting out the fire.



More information:

220-1202, Objective 4.4 - Safety Procedures

<https://professormesser.link/1202040402>

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 which 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 a standard 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:

220-1202, Objective 2.2 - Windows Security Settings

<https://professormesser.link/1202020203>

C42. A Windows administrator needs to define a minimum password length for all network users. Which of the following should be used to complete this task?

- A.** Device Manager
 - B.** Certificate Manager
 - C.** Group Policy Editor
 - D.** Performance Monitor
-

The Answer: **C.** Group Policy Editor

The Group Policy Editor works with Active Directory services to manage almost any aspect of a client system.

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. Certificate Manager

The Certificate Manager is a centralized certificate store for root certificates, trusted publishers, trusted people, and more.

D. Performance Monitor

Performance Monitor gathers long-term statistics and performance metrics from the operating system. Performance monitor will not manage security policies on a system.



More information:

220-1202, Objective 1.4

The Microsoft Management Console

<https://professormesser.link/1202010402>

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.** Organizational Units
-

The Answer: **B.** Least privilege

The principle of least privilege ensures 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 this 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 and allows the administrator to manage the connected Windows devices. Group Policy is not a security principle associated with application rights and permissions.

D. Organization Units

Organizational Units (OUs) are used with Active Directory Domain Services to categorize users, devices, and other components into logical groups.



More information:

220-1202, Objective 2.1 - Logical Security

<https://professormesser.link/1202020103>

C44. A user is receiving this message on their Windows desktop: "The controller does not have enough resources for this device." Which of the following would be the most likely reason for this issue?

- A.** Remote printer has been disabled
 - B.** Wireless network bandwidth exceeded
 - C.** USB endpoints are exceeded
 - D.** The system clock is incorrect
-

The Answer: **C.** USB endpoints are exceeded

USB devices contain buffers called "endpoints," and if those endpoints exceed the capacity of the USB controllers, a "resources exceeded" message will appear. To resolve this issue, move a USB device to a different interface.

The incorrect answers:

A. Remote printer has been disabled

Disabling a remote printer will not commonly show any messages on the Windows desktop.

B. Wireless network bandwidth exceeded

When a wireless network bandwidth is exceeded, the performance of the applications will slow down. Error messages are not commonly displayed on the desktop when a wireless network is busy.

D. The system clock is incorrect

An incorrect system clock will not display a resource error on the Windows desktop.



More information:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

C45. A small company is located in a large office building shared by 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. WPA3 encryption
 - D. SSID suppression
-

The Answer: D. SSID suppression

Disabling the SSID (Service Set Identifier) broadcast 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 list of available connections.

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. WPA3 encryption

WPA3 (Wi-Fi Protected Access version 3) is a security protocol included on 802.11 wireless networks. Enabling WPA3 does not remove the name of the wireless network from the list of available connections.



More information:

220-1202, Objective 2.10 - Securing a SOHO Network
<https://professormesser.link/1202021001>

C46. A manager in the accounting department would like to upgrade to Windows 11, 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.** Image deployment
 - C.** Remote 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 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. Image deployment

An image deployment is a pre-built version of Windows. This image may not include all required applications, and no user data would be contained in an image deployment.

C. Remote 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 an in-place upgrade is occurring.



More information:

220-1202, Objective 1.2 - Upgrading Windows

<https://professormesser.link/1202010202>

C47. A network administrator has modified all wireless access points to use WPA3 instead of WPA2. Which of the following would be a reason for this change?

- A.** Additional frequency choices
 - B.** Lower power consumption
 - C.** Larger usable range
 - D.** Stronger encryption
-

The Answer: **D.** Stronger encryption

The encryption used in WPA3 is the Galois/Counter Mode Protocol and is considered to be a stronger encryption than WPA2.

The incorrect answers:

A. Additional frequency choices

WPA2 and WPA3 are encryption protocols. The available frequencies are a function of the access point standard and not the encryption protocols.

B. Lower power consumption

There's no significant difference in power consumption between WPA2 and WPA3.

C. Larger usable range

As with the frequency choices, WPA2 and WPA3 are encryption protocols and are not associated with the wireless standard running underneath.



More information:

220-1202, Objective 2.3 - Wireless Encryption

<https://professormesser.link/1202020301>

C48. A help desk is receiving reports associated with a group of devices 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.** Metered connection
-

The Answer: **A.** Default gateway

The default gateway is the router providing connectivity 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 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. Metered connection

A metered connection will limit the type and amount of traffic sent over a network connection. Since the pings are working for one device, it's safe to assume the network connections are not metered or restricted.



More information:

220-1202, Objective 1.7 - Windows IP Address Configuration
<https://professormesser.link/1202010703>

C49. A user created some documents on their laptop SSD yesterday, but today has reported a problem accessing the files. They are receiving the message, "You require permission to make changes to this file." Which of the following would be the best next troubleshooting step?

- A. Scan for malware
 - B. Change the boot drive in the BIOS
 - C. Restart the operating system
 - D. Defragment the drive
-

The Answer: A. Scan for malware

Since these files were created by the user and stored on their own laptop, it would be unusual for the permissions to change overnight. Although it's possible this issue could be related to a corruption on the storage drive, it's also important to check for any external factors such as malware or viruses.

The incorrect answers:

B. Change the boot drive in the BIOS

Changing the startup drive would only be useful if multiple operating systems were being used from different storage devices. In this example, no additional operating systems or storage drives were mentioned.

C. Restart the operating system

Although restarting the operating system might recover from a memory leak or temporary issue, a problem with permissions does not usually fix itself with a reboot.

D. Defragment the drive

This laptop is storing files to an SSD, so a defragmentation would not run on this device. Even if this was a traditional hard drive, running a defragmentation would not resolve any problems with file permissions.



More information:

220-1202, Objective 3.4 - Troubleshooting Security Issues
<https://professormesser.link/1202030401>

- 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 which 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 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:

220-1202, Objective 4.7 - Communication
<https://professormesser.link/1202040702>

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:

220-1202, Objective 4.6 - Incident Response

<https://professormesser.link/1202040601>

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.** Secure wireless communication
 - 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) and can encrypt individual files and folders on a drive without encrypting other parts of the file system.

The incorrect answers:

B. Secure wireless communication

It's important to use encryption over wireless networks, and many access points can support the WPA2 (Wi-Fi Protected Access 2) or WPA3 encryption protocols.

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:

220-1202, Objective 2.2 - Windows Security Settings

<https://professormesser.link/1202020203>

C53. A technician has been tasked with updating the BIOS of any Windows device using an older BIOS version. The technician cannot reboot these systems to check the BIOS versions currently in use. Which of the following would be the best way to proceed?

- A. Install the BIOS upgrade regardless of the version
 - B. View BIOS information in Group Policy Editor
 - C. Run a report using Performance Monitor
 - D. Use System Information to view the BIOS version
-

The Answer: D. Use System Information to view the BIOS version

The Windows System Information utility can provide extensive information about hardware, device drivers, software, and more. The BIOS information and version numbers are included in the System Summary screen of System Information.

The incorrect answers:

A. Install the BIOS upgrade regardless of the version

A BIOS upgrade is not a trivial installation, and re-installing the same BIOS version could potentially fail and leave the system unusable. A best practice would only install BIOS upgrades where needed.

B. View BIOS information in Group Policy Editor

The Group Policy Editor is used to define Active Directory policies and permissions. The Group Policy Editor does not contain any information about the UEFI BIOS version numbers.

C. Run a report using Performance Monitor

The Performance Monitor reports can provide extensive long-term information about operating system usage, but it does not provide any details about BIOS versions.



More information:

220-1202, Objective 1.4 - Additional Windows Tools

<https://professormesser.link/1202010403>

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 which 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 instead is 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, 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 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:

220-1202, Objective 4.7 - Professionalism

<https://professormesser.link/1202040701>

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.** Battery backup
 - B.** Cloud storage
 - C.** RADIUS administration servers
 - D.** Image-level backups
-

The Answer: **B.** Cloud storage

Cloud storage would provide a separate and off-site storage of backups, files, and other important documents. One significant advantage of any off-site backup or storage is access to the data if the primary site was to have any type of disaster.

The incorrect answers:

A. Battery backup

Battery backup such as 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 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. However, RADIUS does not provide any data backup or data recovery features.

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:

220-1202, Objective 4.3 - Managing Backups

<https://professormesser.link/1202040301>

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 the shared folders are no longer in the list of available storage drives. The user confirms 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 IP 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 something has been modified with the user or group permissions.

The incorrect answers:

B. User is running untrusted software

Untrusted software can be managed in many different ways, but a share not appearing is not commonly associated with untrusted software. 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

IP (Internet Protocol) filtering allows or prevents a device from communicating across the network. IP filtering is not generally 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:

220-1202, Objective 2.2 - Windows Security Settings

<https://professormesser.link/1202020203>

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.** Corporate license
 - C.** Open-source license
 - D.** End user licensing agreement
-

The Answer: **B.** Corporate 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. Open-source license

An open-source license does not commonly require any payment, so there isn't usually a commercial component or financial arrangement associated with the use of open-source 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:

220-1202, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1202040602>

C58. A client's desktop computer is randomly rebooting throughout the workday without any warnings or error messages. Which of the following would be the best next troubleshooting step?

- A.** Update the system BIOS
 - B.** Reinstall the Windows operating system
 - C.** Boot to Safe Mode and disable all startup applications
 - D.** Perform a full system diagnostic
-

The Answer: **D.** Perform a full system diagnostic

A reboot issue occurring randomly and without any type of repeatable process is difficult to troubleshoot, so it would be useful to know if the hardware in the system is working as expected.

The incorrect answers:

A. Update the system BIOS

There's nothing about this issue which immediately points to a BIOS problem, so updating the UEFI BIOS would not be an initial troubleshooting step.

B. Reinstall the Windows operating system

The user's data is on the drive, and it's not yet known if this issue is related to the hardware or the operating system. Reinstalling Windows would not be the best way to address this reboot issue.

C. Boot to Safe Mode and disable all startup applications

This reboot issue is still a mystery, so making changes to the startup process are not yet warranted.



More information:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

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:

220-1202, Objective 1.8 - macOS Overview
<https://professormesser.link/1202010801>

C60. A laptop in the accounting department has been infected with malware, and the technician has just completed the removal process. Which of the following would be the best way to verify the integrity of the core operating system files?

- A.** Perform a clean Windows install
 - B.** Run the system file check utility
 - C.** Rebuild the Windows profile
 - D.** Roll back the last Windows update
-

The Answer: **B.** Run the system file check utility

Running SFC (System File Check) will scan all of the core operating system files and will verify no changes have been made since the installation. This would be a common check after malware has been removed.

The incorrect answers:

A. Perform a clean Windows install

Replacing everything on the system would provide a trusted operating system, but it would also replace all of the personal files and configurations on the user's computer.

C. Rebuild the Windows profile

A corrupted profile can cause issues during login, but the rebuilding process would not provide any information about the integrity of the operating system.

D. Roll back the last Windows update

Reverting to a previous Windows version or configuration would not provide any information about the operating system or the status of core system files.



More information:

220-1202, Objective 1.5 - Windows Command Line Tools

<https://professormesser.link/1202010501>

C61. A user has noticed 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 without making any changes to the operating system or applications. A diagnostic would provide information about the health of the hardware, 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 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:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

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 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 website’s security certificate is shown because the local computer can’t validate the certificate on the server. The server’s certificate has a specific issuing and expiration date and time, so time drift 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:

220-1202, Objective 3.4 - Troubleshooting Security Issues
<https://professormesser.link/1202030401>

C63. A user's smartphone contains company confidential information which 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.** Locator application
 - B.** Remote wipe
 - C.** Authenticator app
 - 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. Locator application

A locator app would be useful for identifying the location of the phone, but it wouldn't provide any additional security for the data on the device.

C. Authenticator app

An authenticator app would be used to login to a third-party service. Authenticator apps do not provide any security for the data on the local device.

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:

220-1202, Objective 2.8 - Mobile Device Security

<https://professormesser.link/1202020801>

C64. A user would like to configure their local printer to be accessible to anyone on the corporate network. Which of the following would be the best way to configure this connection?

- A.** Configure a VPN connection
 - B.** Create a share name in printer properties
 - C.** Configure a metered connection
 - D.** Use a static IP address
-

The Answer: **B.** Create a share name in printer properties

The printer properties includes a sharing tab with the option to "Share this printer" and create the name for the printer share.

The incorrect answers:

A. Configure a VPN connection

A VPN (Virtual Private Network) creates an encrypted tunnel between two devices or locations. In this example, the printer is used on the internal corporate network so a VPN would not be required.

C. Configure a metered connection

Metered connections are commonly used to reduce data usage, especially over slow or costly links. A metered connection would not be required to share a printer on the corporate network.

D. Use a static IP address

Windows networking does not require a static IP address to share files or printers. Most organizations will use dynamic addressing for all of the user devices.



More information:

220-1202, Objective 1.7 - Windows Network Technologies
<https://professormesser.link/1202010701>

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 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:

220-1202, Objective 2.6 - Removing Malware

<https://professormesser.link/1202020601>

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. APFS
 - C. NTFS
 - D. ext4
-

The Answer: A. exFAT

The exFAT (Extended File Allocation Table) file system is designed for flash drives and is compatible across Windows, Linux, macOS, and other operating systems.

The incorrect answers:

B. APFS

APFS (Apple File System) is used exclusively on macOS and other Apple devices. A flash drive formatted with APFS would not be accessible from the Windows operating system.

C. NTFS

The NTFS (NT File System) file system is the standard for Windows devices. Although it can often be read by other operating systems, it is not completely compatible with the macOS operating system.

D. ext4

The ext4 (Fourth Extended Filesystem) is commonly associated with Linux and Android operating systems. A USB drive formatted with ext4 would not be the best way to transfer files between Windows and macOS.



More information:

220-1202, Objective 1.1 - File Systems

<https://professormesser.link/1202010102>

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 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.** Restart the computer
 - 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 which 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. Restart the computer

It's most likely the Windows patches caused this login problem, so restarting the system would still cause the system to exhibit the same issue.

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 are 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:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

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 and 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." A quick format does not overwrite the data portion of the drive, and recovery software can often restore the remaining data.

C. Drill

A drill will ensure the data cannot be recovered, but it physically damages the drive so it cannot be used by others.



More information:

220-1202, Objective 2.9 - Data Destruction

<https://professormesser.link/1202020901>

C69. A workstation technician manages a training center with 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 computers 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 which 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:

220-1202, Objective 1.2 - Installing Operating Systems

<https://professormesser.link/1202010201>

C70. A user would like to use their smartphone for a payment during checkout at the grocery store, but the smartphone is not seen by the payment system. Which of the following would be the best next troubleshooting step?

- A. Restart the smartphone
 - B. Replace the battery
 - C. Perform a factory reset
 - D. Enable Wi-Fi
-

The Answer: A. Restart the smartphone

There are limited troubleshooting options available for NFC (Near Field Communication) connections, and most smartphones enable the NFC feature by default. If the NFC feature is not seen at all, a restart of the smartphone may enable the functionality.

The incorrect answers:

B. Replace the battery

The NFC features are not directly associated with the battery, and replacing the battery will not resolve this issue.

C. Perform a factory reset

A factory reset would delete all user information from the phone.

Although this may be an option for future troubleshooting, it would not be the best next step for this issue.

D. Enable Wi-Fi

NFC features are not part of the 802.11 Wi-Fi network. Modifying the Wi-Fi configuration and settings will not resolve issues with NFC.



More information:

220-1202, Objective 3.2 - Troubleshooting Mobile Devices

<https://professormesser.link/1202030201>

C71. A technician is troubleshooting a problem with user's laptop and very high utilization, even with no activity on the screen or user input to the operating system. Task Manager shows 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 DDoS attack
 - D.** Network adapter is faulty
-

The Answer: **C.** Laptop is part of a DDoS attack

High CPU utilization, memory use, and network traffic with no user intervention indicates a possible malware infection and participation in a DDoS (Distributed Denial of Service) attack. 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:

220-1202, Objective 2.5 - Denial of Service

<https://professormesser.link/1202020502>

C72. A user's smartphone app shows a splash screen but disappears after a few seconds. Which of the following would be the best way for a technician to view logs and memory statistics for the app?

- A.** Developer mode
 - B.** Cloud storage
 - C.** Jailbreaking
 - D.** Application spoofing
-

The Answer: **A.** Developer mode

Developer mode enables features commonly used by developers. Fortunately, this feature can be used by anyone to help with troubleshooting and information gathering.

The incorrect answers:

B. Cloud storage

Cloud storage is useful for backing up a mobile device, but it doesn't provide any additional statistics or troubleshooting information.

C. Jailbreaking

Jailbreaking is an unsupported method to gain direct access to the smartphone operating system, and it's a direct violation of the software's end user license agreement. Jailbreaking should never be used on a corporate smartphone.

D. Application spoofing

An application which looks legitimate but is instead malicious is an application spoofing attack. Application spoofing does not provide any additional troubleshooting tools.



More information:

220-1202, Objective 3.3

Troubleshooting Mobile Device Security

<https://professormesser.link/1202030301>

C73. A company has created an internal process to ensure 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 which can identify an individual. This information can be 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 improve 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 a process to remove user information, this removal 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, there is most likely a security focus for implementing such a process.



More information:

220-1202, Objective 4.6 - Privacy, Licensing, and Policies
<https://professormesser.link/1202040602>

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 guest account
 - E. Enable file storage quotas
 - F. Enable password complexity
-

The Answers: D. Disable guest account, and
F. Enable password complexity

The only available options associated with server security are those to disable guest accounts and increase the complexity of the passwords. Guest accounts can be exploited, and passwords which 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:

220-1202, Objective 2.7 - Security Best Practices

<https://professormesser.link/1202020701>

C75. A user has purchased a computer which 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 this support is 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:

220-1202, Objective 1.10 - Installing Applications

<https://professormesser.link/1202011001>

C76. A financial services company is upgrading the storage drives in their SAN and need to dispose of one hundred older storage drives. The security administrator would like to permanently disable the drive and guarantee the data on the drives 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 disabled.

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 disable 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 disabled.



More information:

220-1202, Objective 2.9 - Data Destruction

<https://professormesser.link/1202020901>

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 to a battery wholesaler
 - D.** Bury in a landfill
-

The Answer: **A.** Take to a local hazardous waste facility

Batteries contain chemicals which 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 selling 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:

220-1202, Objective 4.5 - Environmental Impacts

<https://professormesser.link/1202040501>

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. Standard operating procedures
 - D. Regulatory compliance documentation
-

The Answer: B. Acceptable use policy

An Acceptable Use Policy (AUP) provides detailed documentation on the correct and expected use of company assets. If someone is dismissed, this document will provide a well-documented set of reasons 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 which must be accepted before the software will install.

C. Standard operating procedures

Standard operating procedures are used by an organization to standardize the process used during the normal course of business. Situations involving downtime or facilities issues are handled using the company's documented set of standard operating procedures.

D. Regulatory compliance documentation

Many companies must comply with local, state, or federal regulations. This compliance is specific to an industry or situation, and may not apply to all companies or individuals.



More information:

220-1202, Objective 4.6 - Privacy, Licensing, and Policies

<https://professormesser.link/1202040602>

C79. A healthcare administrator stores sensitive data on his laptop computer. His desk is in an open area near a busy hallway. Which of the following would add additional security to the administrator's work area?

- A.** Door lock
 - B.** Fingerprint scanner
 - C.** Magnetometer
 - D.** Bollards
-

The Answer: **B.** Fingerprint scanner

A laptop with a fingerprint scanner can limit access to everyone except those individuals with a registered fingerprint.

The incorrect answers:

A. Door lock

This 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. Magnetometer

A magnetometer scans for metal objects and can be used to scan packages, briefcases, or individuals. A magnetometer would not commonly be used to add additional security to a user's laptop.

D. Bollards

A bollard is a barricade used to limit access to an area. This desk is in an open area, so bollards would not be a useful security tool in this case.



More information:

220-1202, Objective 2.1 - Physical Access Security

<https://professormesser.link/1202020102>

C80. A technician has received a help desk ticket asking for help with a broken laptop keyboard. After calling the user, the technician learns the laptop is scheduled to be used for a press event the following day. Which of the following would be the best next step with the ticket?

- A. Refer the ticket to the laptop group
 - B. Escalate the issue with management
 - C. Add the event information to the problem description
 - D. Assign the ticket to the "laptop" category
-

The Answer: B. Escalate the issue with management

The time constraint associated with this issue needs to get the visibility of someone higher in the organization. Escalating the ticket to management will provide additional options for resolution.

The incorrect answers:

A. Refer the ticket to the laptop group

Because of the timeframe associated with this issue, a referral to another group would not provide the urgency required to resolve the problem.

C. Add the event information to the problem description

The event information should certainly be documented, but it would not be the next step given the short timeframe for resolution.

D. Assign the ticket to the "laptop" category

Assigning the ticket to an appropriate category is important for the ticketing process, but it doesn't move the resolution process forward.



More information:

220-1202, Objective 4.1 - Ticketing Systems

<https://professormesser.link/1202040101>

C81. A network administrator has been asked to manage the router configurations at all company locations. Which of the following would be the best choice for this task?

- A. SSH
 - B. VNC
 - C. NFC
 - D. RDP
-

The Answer: A. SSH

SSH (Secure Shell) is a secure protocol for 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. NFC

NFC (Near Field Communication) is a wireless networking technology associated with short-range data transfers. NFC would not be used to manage routers across the network.

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:

220-1202, Objective 4.9 - Remote Access

<https://professormesser.link/1202040901>

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 the browsers on a computer are redirected to a different website, then malware would be a likely suspect. Since 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 web browsing. Some services would be disabled in Safe Mode, but it's unlikely those 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 appears 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 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:

220-1202, Objective 3.4 - Troubleshooting Security Issues
<https://professormesser.link/1202030401>

C83. A technician has just received fifty boxes of used laser printer toner cartridges 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 printer manufacturer
 - C.** Incinerate the cartridges
 - 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 printer manufacturer

The manufacturer of the printer will most likely not be a method of disposal. Hazardous waste and recycling centers can properly dispose of used toner cartridges, and those would be a much better destination than the printer manufacturer.

C. Incinerate the cartridges

Toner cartridges can contain residual toner and chemicals, so they should not be incinerated or subjected to fire.

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.



More information:

220-1202, Objective 4.5 - Environmental Impacts

<https://professormesser.link/1202040501>

C84. A system administrator has been notified 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 for the change control 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 control 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 describing 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:

220-1202, Objective 4.2 - Change Management

<https://professormesser.link/1202040201>

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 detail the donation process.

The incorrect answers:

B. Acceptable use policy

An acceptable use policy is used to understand how company assets should be managed by employees and representatives of the company.

C. Password policy

A password policy is created by the organization's security team to document the complexities required for passwords, the aging of passwords, 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:

220-1202, Objective 4.1 - Asset Management

<https://professormesser.link/1202040102>

- C86.** A technician is troubleshooting a problem on a Linux server and needs to view the real-time CPU and memory utilization for each operating system process. Which of the following would provide this functionality?
- A. dig
 - B. df
 - C. cat
 - D. top
-

The Answer: D. top

The Linux top command is a common method of viewing real-time information about CPU, RAM, and resource utilizations. This information is updated every second by default and can quickly identify highly utilized processes.

The incorrect answers:

A. dig

The dig command is used to query DNS (Domain Name System) servers and view the configuration of the DNS database.

B. df

The df (Disk Free) command displays filesystem information and the free space available for each volume.

C. cat

The cat (Concatenate) command is used to combine files together on the screen or as part of a file.



More information:

220-1202, Objective 1.9- Linux Commands Part 2

<https://professormesser.link/1202010902>

C87. A technician has just installed a new device driver and restarted a Windows laptop, but now the system shows a Windows Stop Error before the login screen is displayed. Which of the following would be the best way to resolve this issue?

- A.** Start in Safe Mode
 - B.** Replace the system memory
 - C.** Reinstall Windows from the original media
 - D.** Perform a full backup
-

The Answer: **A.** Start in Safe Mode

Windows Safe Mode can be used to bypass issues during startup and allow a technician to make changes to the configuration in a minimally functional Windows environment.

The incorrect answers:

B. Replace the system memory

The only change associated with this error is related to a device driver, so replacing the system RAM would not be the most likely resolution.

C. Reinstall Windows from the original media

Reinstalling Windows would most likely resolve this issue, but it could also remove all existing user data and applications and create a much larger problem than simply reverting to a previous driver version.

D. Perform a full backup

Although it's always good to have a backup, this issue would not be resolved by backing up the laptop data.



More information:

220-1202, Objective 3.1 - Troubleshooting Windows

<https://professormesser.link/1202030101>

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 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:

220-1202, Objective 4.4 - Safety Procedures

<https://professormesser.link/1202040402>

C89. A company has configured a server for daily backups, and a full backup is created each Sunday based on the previous incremental backups. Which of the following would best describe this backup strategy?

- A.** Differential
 - B.** GFS
 - C.** Synthetic
 - D.** 3-2-1
-

The Answer: C. Synthetic

A synthetic backup combines a previously taken full backup with a series of updates to build a completely new full backup based on the most recent changes.

The incorrect answers:

A. Differential

A differential backup initially takes a full backup. Subsequent backup sessions contain all changes since the full backup.

B. GFS

GFS is an abbreviation for "Granfather-Father-Son." An example of this backup strategy might describe three different backup rotations for each month (grandfather), each week (father), and each day (son).

D. 3-2-1

The 3-2-1 backup rule states three copies of data should always be available, two different types of media should be used, and one copy of the backup should be stored offsite.



More information:

220-1202, Objective 4.3 - Managing Backups

<https://professormesser.link/1202040301>

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.

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:

220-1202, Objective 2.5 - Social Engineering

<https://professormesser.link/1202020501>

Continue your journey on
ProfessorMesser.com:



Professor Messer's
CompTIA A+

CORE 2 220-1202

**Professor Messer's CompTIA
A+ Training Course**

Monthly A+ Study Group Live Streams

24 x 7 Live Chat

**Professor Messer's CompTIA
A+ Course Notes**

Discounted Vouchers



Professor Messer's CompTIA A+ **CORE 2** 220-1202 Practice Exams

The 220-1202 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