220-1002.62q

220-1002

CompTIA A+ Certification Exam: Core 2

Exam A

QUESTION 1
A technician arrives on site to find that two users who have the same model on Android smartphone are having the same issue with a specific application. Whenever they attempt to launch the application, it fails and gives an error message. Which of the following should the technician do FIRST?

A. Reinstall the application
B. Roll back the application to the earlier version
C. Clear the application cache
D. Update the OS of the smartphones

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
An administrator is setting up a Windows terminal server. Which of the following settings should the administrator modify to increase server security? (Select two.)

A. Change the default access port
B. Enforce password complexity
C. Put the terminal server into the router's DMZ
D. Disable logon time restrictions
E. Block all unused ports on the LAN smart switch
F. Use the local client certificate for server authentication

Correct Answer: CE

Section: (none)
Explanation

Explanation/Reference:
QUESTION 3
A small office's wireless network was compromised recently by an attacker who brute forced a PIN to gain access. The attacker then modified the DNS settings on the router and spread malware to the entire network.
Which of the following configurations MOST likely allowed the attack to take place? (Select two.)

A. Guest network
B. TKIP
C. Default login
D. Outdated firmware
E. WPS
F. WEP

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A technician receives an invalid certificate error when visiting a website with port 443 enabled. Other computers on the same LAN do not exhibit this symptom. Which of the following needs to be adjusted on the workstation to fix the issue?

A. Date and time
B. UEFI boot mode
C. Logon times
D. User access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5

Which of the following is the amount of memory a user is limited to with a 32-bit version of Windows?

A. 2GB
B. 4GB
C. 8GB
D. 16GB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6

A user's phone contains customer's PII. The user cannot have the phone automatically wiped because the data is very valuable. Which of the following is the BEST method of securing the phone?

A. Fingerprint lock
B. Passcode lock
C. Swipe lock
D. PIN lock

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

Which of the following devices are MOST likely to have a grounding wire attached to them based on the manufacturer's design? (Select two.)

A. UPS
B. Server rack
C. PoE phone
D. Desktop printer

E. Modem

F. Patch panel

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

A technician is installing a private PC in a public workspace. Which of the following password practices should the technician implement on the PC to secure network access?

A. Remove the guest account from the administrators group

B. Disable single sign-on

C. Issue a default strong password for all users

D. Require authentication on wake-up

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

Joe, an employee, took a company-issues Windows laptop home, but is having trouble connecting to any of the shares hosted on his home media server.
Joe has verified he is connected to the Internet.
Which of the following would explain why Joe cannot access his personal shares?

A. An IP conflict is present

B. A corporate VPN is enabled

C. A firewall exception must be set

D. HomeGroup must be enabled

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
QUESTION 10
Joe, a customer, has informed a Tier 2 help desk technician that a computer will not boot up. After about ten minutes of troubleshooting, Joe is increasingly concerned and claims that the technician is wasting his time because he has already tried everything that has been suggested. Which of the following should the technician do?

A. Since Joe is concerned about time, suggest calling back later when Joe has more time to troubleshoot
B. Record the call and send it to the local intranet for future technicians to learn how to deal with calls like this one
C. Ask more open-ended questions to see if the issue can be narrowed down in order to properly identify the issue and save time
D. Inform the customer that there is a troubleshooting script that must be followed to get the issue resolved

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A technician has been asked to recommend antivirus software for a home PC, but the user does not want to pay for a license.
Which of the following license type should the technician recommend?

A. Open license
B. Personal license
C. Corporate license
D. Enterprise license

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12

Joe, a systems administrator, is setting up a risk management plan for the IT department. Part of the plan is to take daily backups of all servers. The server backups will be saved locally to NAS.

Which of the following can Joe do to ensure the backups will work if needed?

A. Frequently restore the servers from backup files and test them
B. Configure the backups to restore to virtual machines for quick recovery
C. Set up scripts that automatically rerun failed backup jobs
D. Set up alerts to let administrators know when backups fail
E. Store copies of the backups off-side in a secure datacenter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A SOHO customer has recently experienced a major hurricane. The customer has no backups and has lost all data and hardware associated with the company. The customer calls a contractor to assist in the rebuilding process and needs suggestions on the best way to prevent this from happening again. Which of the following recommendations should the contractor give to the customer? (Select two.)

A. Backup testing
B. Cloud storage
C. Local storage backups
D. Data recovery
E. Hot site
F. Waterproof devices

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

A technician is running updates on a Windows PC. Some of the updates install properly, while others appear as failed. While troubleshooting, the technician restarts the PC and attempts to install the failed updates again. The updates continue to fail. Which of the following is the FIRST option to check?

A. Visit the Microsoft Update website to see if there is an issue with a specific update
B. Look up the error number associated with the failed update
C. Look at the system Event Viewer to find more information on the failure
D. Download the failed update to install manually

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A technician has identified malware on a user's system. Which of the following should the technician do NEXT according to malware removal best practices?

A. Enable System Restore and create a restore point so no data is lost
B. Educate the user about how to avoid malware in the future
C. Update the antivirus software and run a full system scan
D. Move the infected system to a lab with no network connectivity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A user's Windows laptop has become consistently slower over time. The technician checks the CPU utilization and sees that it varies between 95% and 100%. After the technician closes some running applications, the CPU utilization drops to approximately 20%, and the laptop runs much faster. The next day the same user calls again with the same problem. Which of the following is a tool the technician can use to resolve the issue?

A. Task Manager
B. MSTSC

C. MSConfig
D. PerfMon

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 17
A user is requesting a solution that will prevent file corruption and ensure a graceful shutdown while providing at least one hour of uptime in case of extreme weather conditions. Which of the following should a technician recommend?

https://vceplus.com/

A. Uninterruptible power supply
B. Surge protector
C. Power strip
D. Power distribution unit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which of the following installation types would require the use of an answer file to install the OS?

A. Unattended
B. Clean
C. Repair
D. Upgrade

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 19
A MAC user's operating system became corrupted, and files were deleted after malware was downloaded. The user needs to access the data that was previously stored on the MAC. Which of the following built-in utilities should be used?

A. Time Machine
B. Snapshot
C. System Restore
D. Boot Camp

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A manager with a restricted user account receives the following error message:

```
Windows Update cannot currently check for updates because the service is not running.
```

The manager contacts the help desk to report the error. A technician remotely connects to the user's computer and identifies the problem. Which of the following should the technician do NEXT?

A. Reboot the computer
B. Restart the network services
C. Roll back the device drivers

D. Rebuild the Windows profiles

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
A SOHO technician recently moved some data from one server to another to increase storage capacity. Several users are now reporting they cannot access certain shares on the network. When the users attempt to access the shares, they get the following error: `Access Denied`. The technician confirms the users are all in the proper security groups and have the proper access, but they are still unable to access the shares. Which of the following are the MOST likely reasons for these issues? (Select two.)

A. Administrative share permissions
B. Mapped drives
C. Group Policy hours restriction
D. Denied write/delete permissions
E. Disabled proxy settings

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
With which of the following types is a man-in-the-middle attack associated?

A. Brute force
B. Spoofing
C. DDoS
D. Zero-day

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
An employee is unable to view in-office network folders while working at home. Which of the following is the MOST likely cause of the problem?

A. Untrusted software
B. Outdated antivirus
C. MDM policies
D. Inactive VPN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A network administrator notifies a technician that the company is experiencing a DDoS attack. Several internal Windows PCs are the source of the traffic. The network administrator gives the technician the Windows computer names and states they be scanned and cleaned immediately. With which of the following types of infections are the PCs MOST likely infected? (Select two.)

A. Spyware
B. Zombies
C. Virus
D. Ransomware
E. Worm
F. Botnet

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Ann, a user, is attempting to log in to her email service form a third-party email client on her phone. When Ann enters her usual username and password, she receives an error message saying the credentials are invalid. Ann then decides to reset her email password, but after the reset, the new credentials still do not work in the third-party email client.
Which of the following settings or features is responsible for the problems Ann is experiencing?

A. Full device encryption
B. Account lock
C. Multifactor authentication
D. Strong password requirements

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Joe, a user, returns his computer to the technician who performed a virus removal on it the week before. Joe states that several symptoms have returned.
Which of the following should the technician have covered previously as part of the original repair?

A. End-user education
B. Pre-installation environment cleaning
C. Disabling of System Restore
D. Infected system quarantine

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following steps should a technician take FIRST to prevent an electrical hazard when repairing a PC?

A. Put on an ESD strap.

B. Place components on an ESD mat
C. Disconnect the power before servicing the PC
D. Place the PC on a grounded work bench

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Ann, a user, calls the help desk regarding an issue on her laptop. While working remotely, she appears to be connecting to WiFi but is unable to retrieve her corporate email. The wireless name is listed as "ConnectMe" and appears as unsecure. Which of the following should the help desk perform to fix the issue?

A. Remote into Ann's system and restart the wireless adapter
B. Ask Ann to open a browser and watch for a redirect page
C. Advice Ann to pug an Ethernet cable into her laptop
D. Direct Ann to run an antivirus program on her laptop

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A project team is organized to implement a new wireless solution for a school. The team has already done the network diagrams and knows the locations that will need to be addressed in the project. The team is in the process of creating an SOW for the project as a whole and needs to add the critical pieces to the SOW to complete it and move to the next stage.
Which of the following would the project team MOST likely add to the SOW?

A. Risk analysis
B. Plan to change
C. Backout plan
D. Change board approvals

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
An end user's PC is taking a long time to boot. Which of the following operations would be the BEST to resolve this issue with minimal expense? (Select two.)

A. Remove applications from startup
B. Defragment the hard drive
C. Install additional RAM
D. Install a faster hard drive
E. End the processes in Task Manager
F. Run the Disk Cleanup utility

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A technician is PXE booting a computer. Which of the following is the technician MOST likely performing on the computer?

A. Image deployment
B. Multiboot configuration
C. In-place upgrade
D. System repair

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Ann, an employee at a company, calls the help desk to report issues logging on to a vendor's website. Joe, the technician, is able to log in successfully with his credentials before going to Ann's office. However, when he attempts to log in from Ann's office, Joe experiences the same issue. Ann asks Joe questions about the new software installed on the laptop from the pop-up notification.
Which of the following are the NEXT steps Joe should take to resolve the issue? (Select two.)

A. Ask Ann for her credentials to verify and log on to the vendor's website from Ann's laptop
B. Verify Ann's laptop has the correct browser settings
C. Check all browser cached files on Ann's laptop and log on to another vendor's website
D. Attempt to log on to another vendor's website from Ann's laptop
E. Ask Ann about the notification and review the installed programs
F. Reinstall the browser, reboot the laptop, and check the vendor's website again

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Ann, a user, has purchased a new Android phone and is attempting to access a public hotspot. When she gets a message indicating the page cannot be displayed. She notices there is a "?" in the radio icon in the toolbar. She has verified Bluetooth is active, airplane mode is off, and tethering is turned on. She uses the cell phone to call a technician for assistance. Which of the following is the MOST likely issue Ann is experiencing?

A. There is unauthenticated wireless connectivity
B. She has exceeded the data allowance
C. The phone is only 3G capable
D. It is an unrooted phone
E. The SIM card was not activated
F. A data plan was not purchased

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A small business has an open wireless network so vendors can connect to the network without logging in. The business owners are concerned that a nearby company is connecting and using the wireless connection without permission. If the small business requires that the network remain open, which of the following configuration settings should be changed to address these concerns?

A. Default SSID
B. MAC filtering
C. Power levels
D. Content filtering
E. Firewall

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 35
A technician is working on a user's workstation and notices a lot of unknown processes running in the background. The user informs the technician that an application was recently downloaded from the Internet.
Which of the following types of infection does the user MOST likely have?

A. Rootkit
B. Keylogger
C. Trojan
D. Ransomware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36

A small business has an open WiFi network for employees but does not want customers to connect to the access point. A technician has been dispatched to address the business's concerns. Which of the following configuration settings should the technician change to satisfy the requirements of the business? (Select two.)

A. Default SSID
B. MAC filtering
C. NAT
D. QoS
E. Signal strength
F. Encryption

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
QUESTION 37
A computer becomes infected with malware, which manages to steal all credentials stored on the PC. The malware then uses elevated credentials to infect all other PCs at the site. Management asks the IT staff to take action to prevent this from reoccurring. Which of the following would BEST accomplish this goal?

A. Use an antivirus product capable of performing heuristic analysis
B. Use a host-based intrusion detection system on each computer
C. Disallow the password caching of accounts in the administrators group
D. Install a UTM in between PC endpoints to monitor for suspicious traffic
E. Log all failed login attempts to the PCs and report them to a central server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following technologies is used by malicious employees to obtain user passwords?

A. Main-in-the-middle

B. Phishing
C. Tailgating
D. Shoulder surfing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A user reports that when opening a web browser, the initial page loads to a search engine the user does not recognize. When the user performs searches on the site, the results are often irrelevant, and there are many pop-ups. Which of the following should a technician do to resolve these issues? (Choose two.)

A. Reset the user's browser to default settings
B. Delete the user's cached images, temporary files, and cookies
C. Reboot the user's computer and install a secondary antivirus
D. Convince the user to use a different web browser that is currently unaffected
E. Download the update to the user's web browser of choice
F. Remove any unapproved applications from the user's startup items

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A technician is in the process of upgrading Windows 8 to Windows 10. The technician needs to make sure all of the applications, user profiles, documents, and PST files are preserved. Which of the following methods would the technician MOST likely perform on the computer?

A. Unattended installation
B. Refresh upgrade
C. Clean installation
D. In-place upgrade

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following is the MOST secure wireless security protocol?

A. AES
B. WPA
C. WPA2
D. WEP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Corporate management is concerned about the security of the company's mobile phones, in the event they are lost or stolen. Management instructs the IT staff to ensure the data on the devices is not accessible by unauthorized users. Which of the following would provide the BEST level of protection in this scenario? (Choose two.)

A. Use full device encryption
B. Enable a pattern lock
C. Implement remote wipe features
D. Use device lockout policies
E. Require complex administrator passwords
F. Disable unknown application installations

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A technician repaired a laptop for a customer. The customer then complained the repair took too long and questioned the steps the technician took to fix the problem. Which of the following should the technician do NEXT?

A. Provide documentation of the repair to the customer
B. Allow the customer to voice concerns and post the story to social media later
C. Inform the customer the job is done and return to the office
D. Defend each step and why it was necessary

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 44
A technician received 300 old desktops following a recent computer upgrade. After taking inventory of the old machines, the technician must destroy the data on the HDDs. Which of the following would be the MOST effective method to accomplish this task?

A. Drill
B. Hammer
C. Low-level format
D. Degaussing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
A user reports malware activity on an isolated workstation used for testing. It is running an end-of-life OS, and a USB drive is the only method used to transfer files. After removing the malware and replacing the USB drive with a brand new one, the technician gives the approval to use the equipment. The next day the user reports the same malware activity is present after powering on the system. Which of the following did the technician forget to do to prevent reinfection?

A. Connect to the network and update the OS with the latest security patches
B. Scan and clean the USB device used to transfer data from the equipment
C. Disable System restore and remove all restore points from the system
D. Update the local antivirus and set it to scan automatically every evening

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A corporate network was recently infected by a malicious application on a flash drive that downloaded sensitive company files and injected a virus, which spread onto the network. Which of the following best practices could have prevented the attack?

A. Implementing strong passwords
B. Changing default credentials
C. Disabling AutoRun
D. Removing Guest account
E. Encrypting data

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following technologies can be utilized in a wireless network environment to provide secure SSO access for WiFi and network resources?

A. WPA2
B. AES
C. MAC filtering
D. RADIUS
E. WPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A technician recently installed a new secondary hard drive in a Windows 10 desktop. After the installation, the computer displayed the following error message: `No Operating System Found`. However, after unplugging the new hard drive, the error message no longer appeared. The technician then reconnected the new drive to continue troubleshooting. Which of the following steps should the technician take NEXT?

A. Reboot into safe mode
B. Check the boot order
C. Format the drive
D. Perform Windows Recovery
E. Run the `chkdsk` command

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
After a security audit, a technician is tasked with implementing new measures to help secure company workstations. The new policy states that all workstations must be signed off at night, a password is necessary to boot the computer, and encryption must be enabled. Which of the following features should the technician implement to BEST meet these requirements? (Choose three.)

A. Screen locks
B. Screensaver passwords
C. UEFI passwords
D. Login time restrictions
E. Strong passwords
F. Multifactor authentication
G. BitLocker
H. Credential Manager
I. Smart card
J. Biometric authentication

Correct Answer: ABG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A new business will be using credit cards in a physical location as well as its web presence. Which of the following does the business need?
A. PHI certification
B. PCI compliance
C. POTS implementation
D. PII filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
A technician has been dispatched to resolve a malware problem on a user's workstation. The antivirus program discovered several hundred potential malware items on the workstation and removed them successfully. The technician decides to schedule daily scans on the system, enables System Restore, and creates a restore point. Which of the following should the technician do NEXT?

A. Run the scan again to ensure all malware has been removed
B. Quarantine the infected workstation from the network
C. Install all of the latest Windows Updates to patch the system
D. Educate the user on safe browsing practices

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
A user's smartphone is experiencing limited bandwidth when at home. The user reports to a technician that the device functions properly when at work or in the car. Which of the following troubleshooting steps should the technician take NEXT?

A. Reset the device's network settings
B. Check the data usage statistics on the device
C. Verify the SSID with which the device is associated
D. Run any pending application or OS updates

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following would a technician use to store memory chips from a laptop safely after an upgrade?

A. Mylar bags
B. Cardboard boxes
C. Antistatic containers
D. Paper envelopes

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
A user notices recent print jobs are not printing to the local printer despite printing fine yesterday. There are no errors indicated on the taskbar printer icon. Which of the following actions should the user take FIRST?

A. Check to ensure the printer selected is the default printer
B. Check the status of the print server queue
C. Cancel all documents and print them again
D. Check that the printer is not offline print mode

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following provide the MOST security for PCs and mobile devices? (Choose two.)

A. Access control lists
B. Multifactor authentication
C. Organizational unit
D. Trusted software sources
E. Data loss prevention
F. Pre-shared key

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A customer purchased a 3TB HDD to use with a Windows 7 PC and wants to have letter "J" assigned only to the drive. Which of the following types of partitioning should be performed to give the customer full use of the 3 TB drive?

A. GPT
B. Dynamic
C. Basic
D. Extended

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Users notify the help desk of an email that was just received. The email came from the help desk's email address and asked the users to click on an embedded link. This email is BEST described as:

A. phishing.
B. zombie.
C. whaling.
D. spoofing.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A user's corporate email is missing the shared inbox folders that were present before the user went on vacation. The technician verifies the user is connected to the domain and can still send and receive email. Which of the following is MOST likely causing the missing folders issue?

A. The Internet security options have changed
B. The operating system updates have changed

C. The network directory permissions have changed

D. The user account permissions have changed

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
During the firmware upgrade of a web server, a power outage occurred. The outage caused a failure within the upgrade. Which of the following plans must be implemented to revert back to the most recent version of the firmware?

A. Backout plan

B. Contingency plan

C. Alternative plan

D. Backup plan

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 60
A new company policy states that all end-user access to network resources will be controlled based on the users' roles and responsibilities within the organization. Which of the following security concepts has the company just enabled?

A. Certificates

B. Least privilege

C. Directory permissions

D. Blacklists

Correct Answer: B
Section: (none)
Explanation

QUESTION 61

A technician performs a virus cleaning on a computer that has been redirecting all browsers to a phishing website. System Restore was turned off before the cleaning. The technician runs the machine through several scanners, and then tests for redirection. A smaller number of sites are still redirecting to the phishing website. The antivirus software correctly blocks the website. Which of the following should the technician do NEXT?

A. Check the contents of the hosts file
B. Do a System Restore to a date before the infection
C. Rerun the antivirus scan with higher sensitivity
D. Rebuild the OS on the machine

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62

A user calls a technician to report issues when logging in to a vendor's website. The technician is able to log in successfully before going to the office. However, the technician is unable to log in when in the user's office. The user also informs the technician of strange pop-up notifications. Which of the following are the MOST likely causes of these issues? (Choose two.)

A. System files have been deleted
B. Proxy settings are configured improperly
C. The OS has been updated recently
D. There are disabled services on the vendor website
E. Program file permissions have changed recently
F. There is a rogue anti-malware program

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference: