DUMPSARENA

CompTIA A+ Certification Exam: Core 2

CompTIA 220-1202

Version Demo

Total Demo Questions: 15

Total Premium Questions: 290

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened white browsing the internet. The technician does not recognize the interface with which the antivirus message is presented. Which of the following is the NEXT step the technician should take?

A. Shut down the infected computer and swap it with another computer

B. Investigate what the interface is and what triggered it to pop up

C. Proceed with initiating a full scan and removal of the viruses using the presented interface

D. Call the phone number displayed in the interface of the antivirus removal tool

ANSWER: B

Explanation:

The technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool12

Shutting down the infected computer and swapping it with another computer is not necessary at this point12

The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

QUESTION NO: 2

A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

A. The technician presses the Ctrl+Alt+Del keys to open the Force Quit menu, selects the frozen application in the list, and clicks Force Quit.

B. The technician clicks on the frozen application and presses and holds the Esc key on the keyboard for 10 seconds Which causes the application to force quit.

C. The technician opens Finder, navigates to the Applications folder, locates the application that is frozen in the list, right-clicks on the application, and selects the Force Quit option.

D. The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit.

ANSWER: D

Explanation:

The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit. This is the most common method of force quitting a program in macOS. This can be done by clicking on the Apple icon

in the top left of the screen, selecting Force Quit, selecting the frozen application in the list, and then clicking Force Quit. This will force the application to quit and the spinning round cursor will disappear.

QUESTION NO: 3

Which of the following provide the BEST way to secure physical access to a data cento server room? (Select TWO).

A. Biometric lock

B. Badge reader

C. USB token

D. Video surveillance

E. Locking rack

F. Access control vestibule

ANSWER: A B

Explanation:

A biometric lock requires an authorized user to provide a unique biometric identifier, such as a fingerprint, in order to gain access to the server room. A badge reader requires an authorized user to swipe an access card in order to gain access. Both of these methods ensure that only authorized personnel are able to access the server room. Additionally, video surveillance and access control vestibules can be used to further secure the server room. Finally, a locking rack can be used to physically secure the servers, so that they cannot be accessed without the appropriate key.

QUESTION NO: 4

A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

A. Configure the network as private

B. Enable a proxy server

C. Grant the network administrator role to the user

D. Create a shortcut to public documents

ANSWER: A

Explanation:

The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

QUESTION NO: 5

A user reports that text on the screen is too small. The user would like to make the text larger and easier to see. Which of the following is the BEST way for the user to increase the size of text, applications, and other items using the Windows 10 Settings tool?

A. Open Settings select Devices, select Display, and change the display resolution to a lower resolution option

B. Open Settings, select System, select Display, and change the display resolution to a lower resolution option.

C. Open Settings Select System, select Display, and change the Scale and layout setting to a higher percentage.

D. Open Settings select Personalization, select Display and change the Scale and layout setting to a higher percentage

ANSWER: C

Explanation:

Open Settings, select System, select Display, and change the Scale and layout setting to a higher percentage123

Reference: 4. How to Increase the Text Size on Your Computer. Retrieved from https://www.laptopmag.com/articles/increase-text-size-computer 5. How to Change the Size of Text in Windows 10. Retrieved from https://www.howtogeek.com/370055/how-to-change-the-size-of-text-in-windows-10/ 6. Change the size of text in Windows. Retrieved from https://support.microsoft.com/en-us/windows/change-the-size-of-text-in-windows-1d5830c3-eee3-8eaa-836b-abcc37d99b9a

QUESTION NO: 6

A user is being directed by the help desk to look up a Windows PC's network name so the help desk can use a remote administration tool to assist the user. Which of the following commands would allow the user to give the technician the correct information? (Select TWO).

A. ipconfig /all

B. hostname

C. netstat /?

D. nslookup localhost

E. arp —a

F. ping :: 1

ANSWER: A B

Explanation:

The user can use the following commands to give the technician the correct information: ipconfig /alland hostname1. The ipconfig /allcommand displays the IP address, subnet mask, and default gateway for all adapters on the computer 1. The hostnamecommand displays the name of the computer 1.

QUESTION NO: 7

A manager reports that staff members often forget the passwords to their mobile devices and applications. Which of the following should the systems administrator do to reduce the number of help desk tickets submitted?

A. Enable multifactor authentication.

B. Increase the failed log-in threshold.

C. Remove complex password requirements.

D. Implement a single sign-on with biometrics.

ANSWER: A

Explanation:

Multifactor authentication (MFA) is a security measure that requires users to provide multiple pieces of evidence when logging in to an account or system. This can include a combination of something the user knows (e.g. a password or PIN), something the user has (e.g. a security token or smartphone) and something the user is (e.g. biometrics such as a fingerprint or face scan). By enabling MFA, the systems administrator can ensure that users are required to provide multiple pieces of evidence when logging in, making it more difficult for unauthorized users to gain access to the system. This can help reduce the number of help desk tickets submitted due to forgotten passwords.

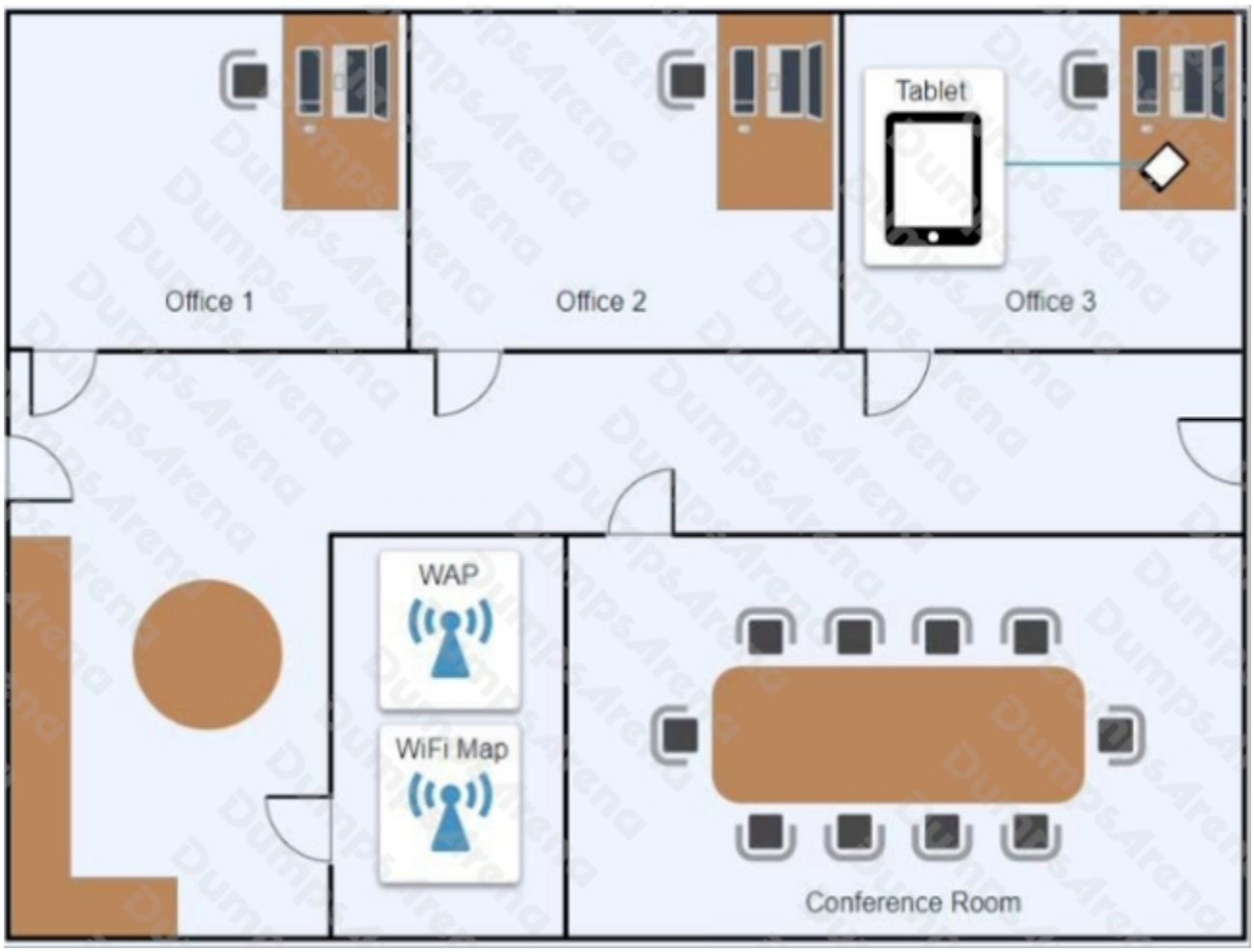
QUESTION NO: 8 - (SIMULATION)

Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect it to the company's wireless network. All the corporate laptops are connecting without issue. She has asked you to assist with getting the device online.

INSTRUCTIONS

Review the network diagrams and device configurations to determine the cause of the problem and resolve any discovered issues.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Tablet
Office 1
Office 2
Office 3
WAP
WiFi Map
Conference Room


Settings
WiFi
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
802.11 None
SSID ANNHOME
Saved Networks
Frequency None
WIRELESS SECURITY MODE
Security Mode None
Passphrase Enter Value
Forget All Networks and Settings


Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
42%
‹ Wi-Fi
802.11
b/g
a
ac

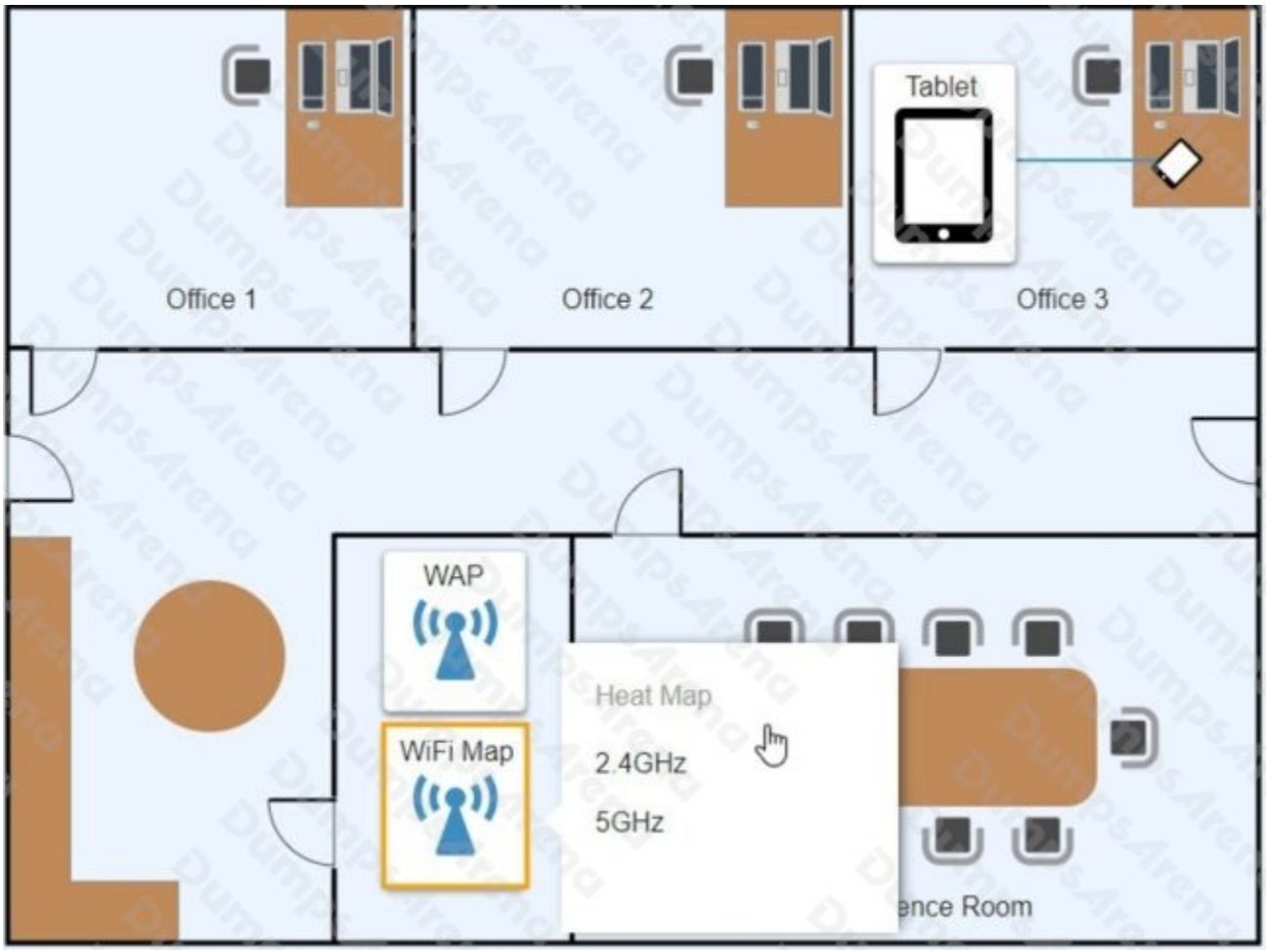

Settings
Settings
Airplane Mode
Wi-Fi
None
Bluetooth
On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
Wi-Fi
SSID
BYOD
DEFAULT
CORP
ANNHOME


Settings
Settings
Airplane Mode
Wi-Fi
None
Bluetooth
On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
42%
< Wi-Fi
Saved Networks
ANNHOME
COFFEESHOPPE
PAMSHOUSE


Settings
Settings
Airplane Mode
Wi-Fi
None
Bluetooth
On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
42%
Wi-Fi
Frequency
2.4GHz
5GHz


Settings
Settings
Airplane Mode
Wi-Fi
None
Bluetooth
On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
42%
‹ Wi-Fi
Security Mode
OPEN
WEP
WPA
WPA2


Settings
Site
Wireless Networks
Networks
Guest Control
Admins
User Groups
VOIP
Controller
Cloud Access
Maintenance
Wireless Networks
SSID
Frequency
Security
Totally Secure!
CORP
2.4GHz/5GHz
WPA2
Corpsecure1
BYOD
2.4GHz/5GHz
WPA-PSK
TotallySecure!
Create New Wireless Network



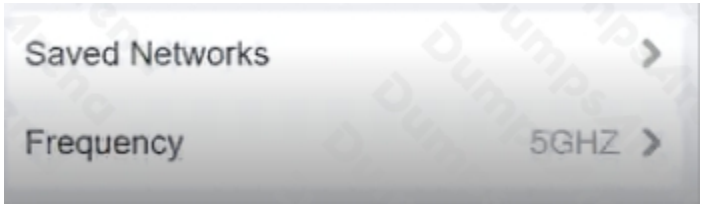
ANSWER: Seethebelow:

Explanation:

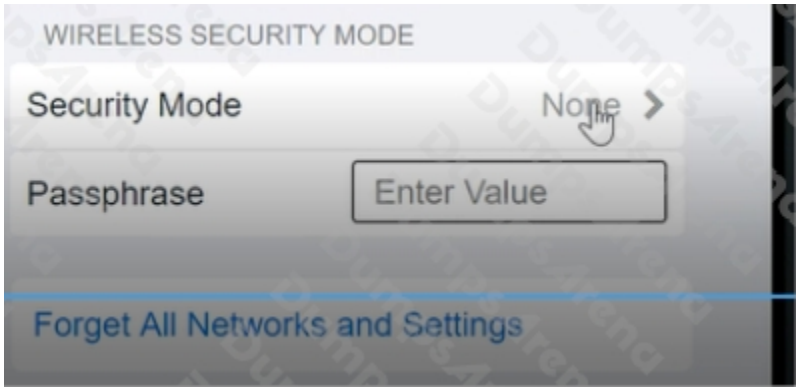
Click on 802.11 and Select ac

Click on SSID and select CORP

Click on Frequency and select 5GHz



At Wireless Security Mode, Click on Security Mode



Select the WPA2

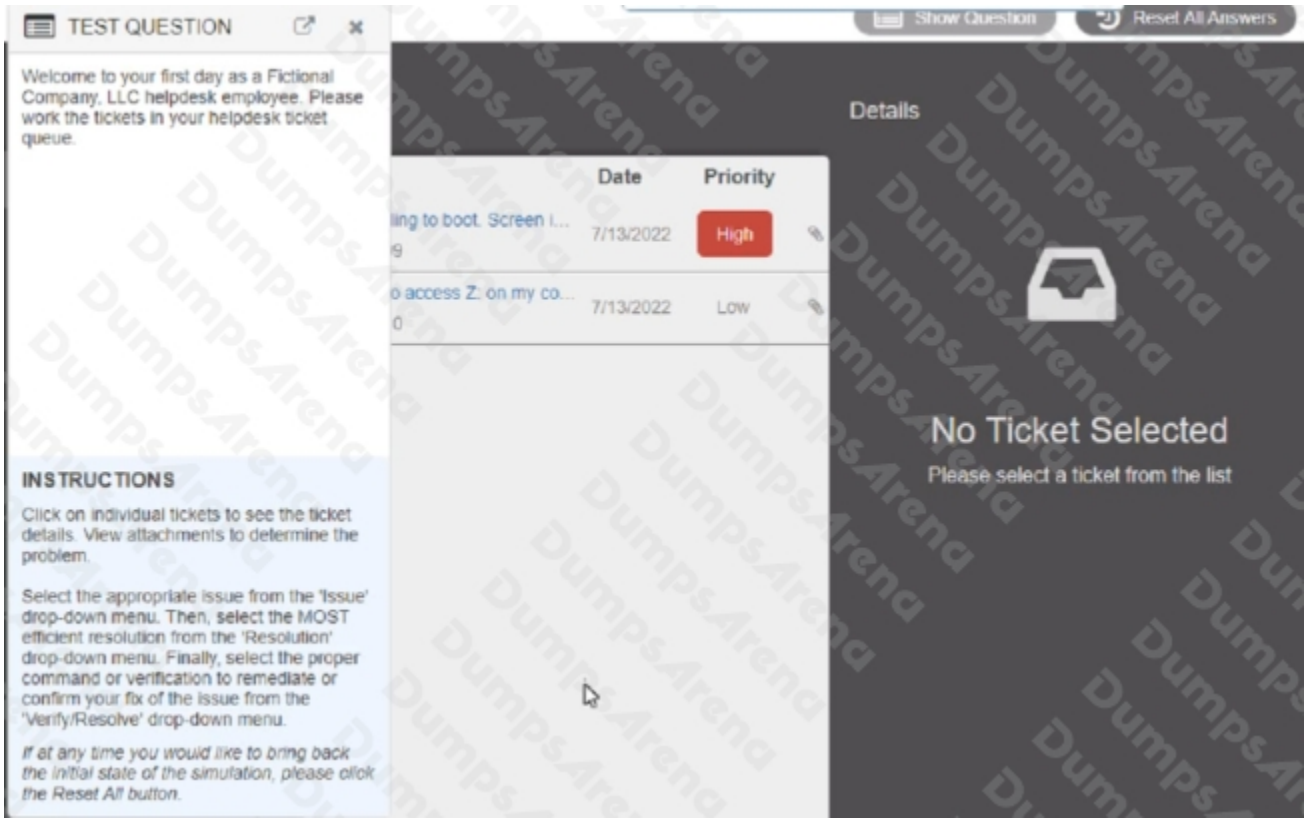
Ann needs to connect to the BYOD SSID, using 2.4GHZ. The selected security method chose should be WPA PSK, and the password should be set to TotallySecret.

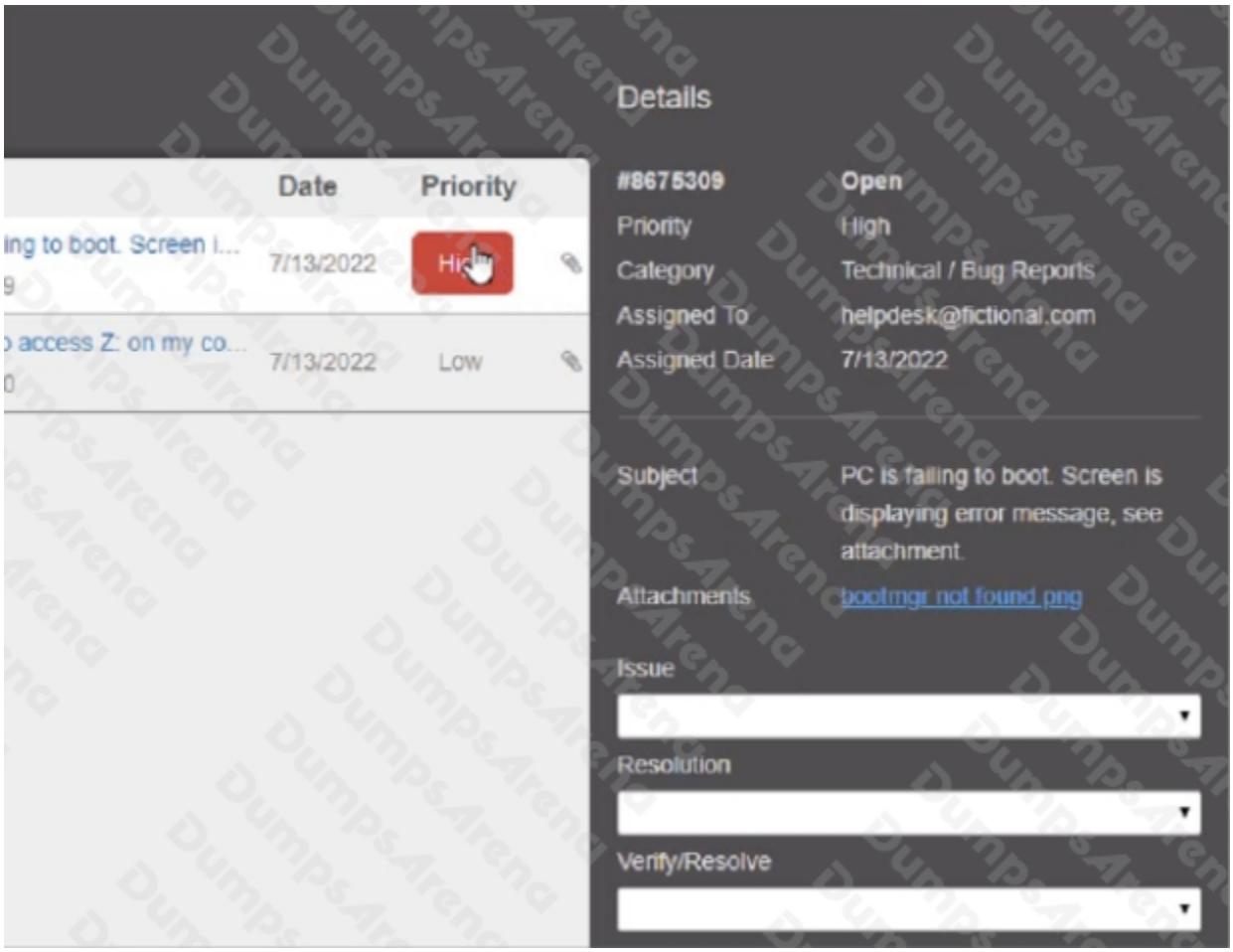
QUESTION NO: 9 - (HOTSPOT)

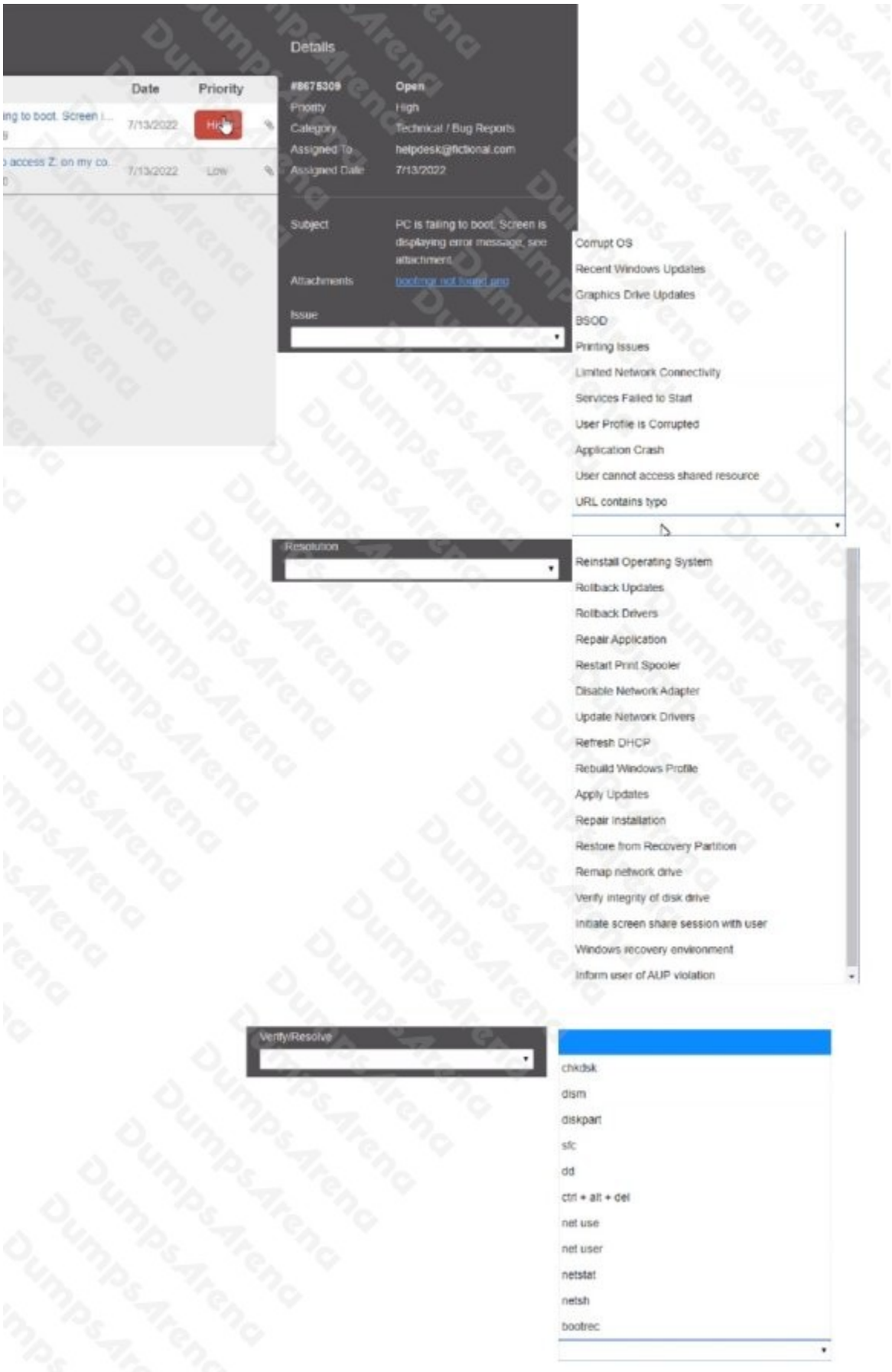
Welcome to your first day as a Fictional Company. LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

Click on individual tickers to see the ticket details. View attachments to determine the problem.

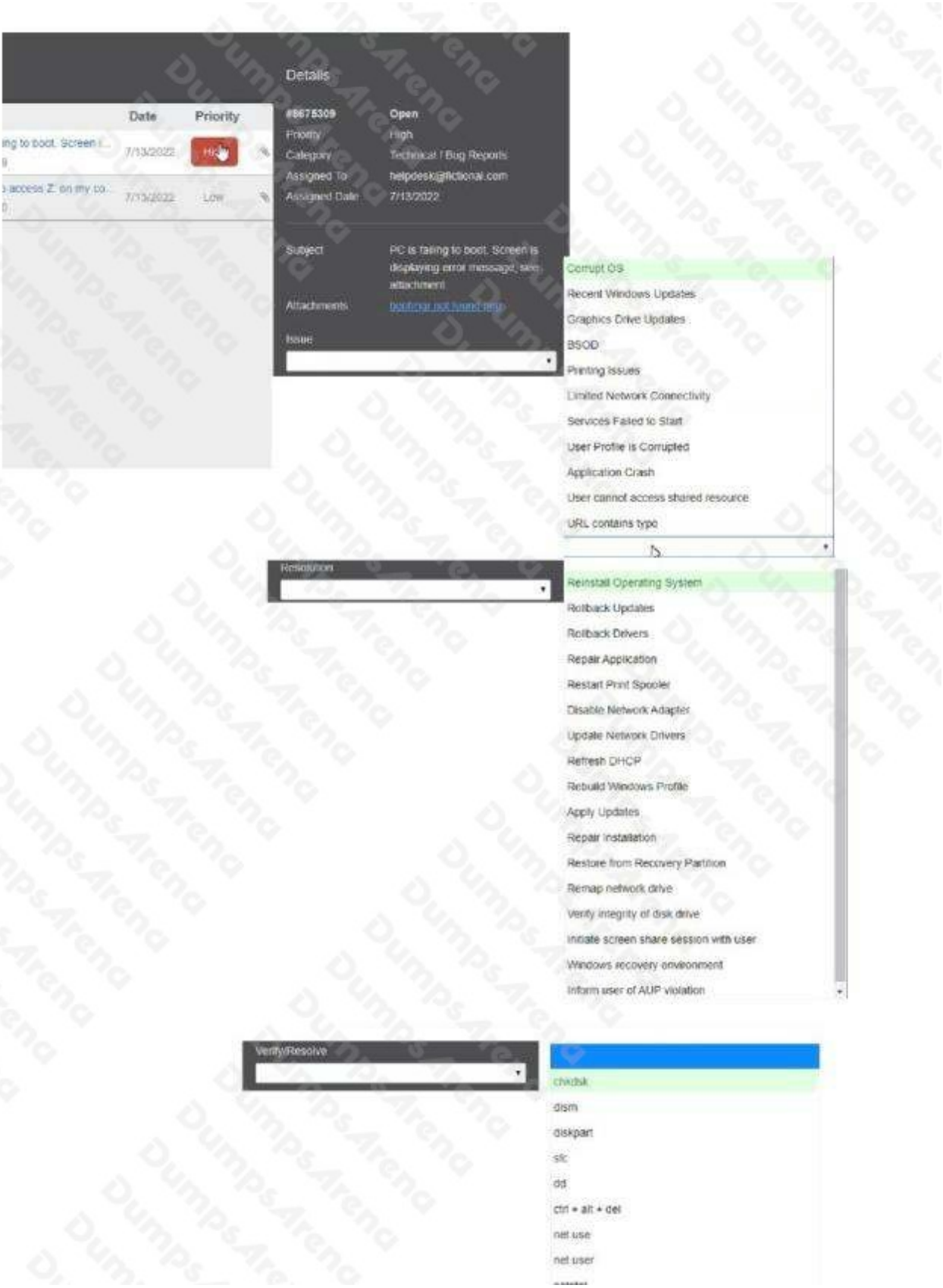
Select the appropriate issue from the 'issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify Resolve drop-down menu.


TEST QUESTION
Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.
INSTRUCTIONS
Click on individual tickets to see the ticket details. View attachments to determine the problem.
Select the appropriate issue from the 'Issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the 'Verify/Resolve' drop-down menu.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Show Question
Reset All Answers
Details
Date
Priority
ling to boot. Screen i...
7/13/2022
High
o access Z: on my co...
7/13/2022
Low
No Ticket Selected
Please select a ticket from the list

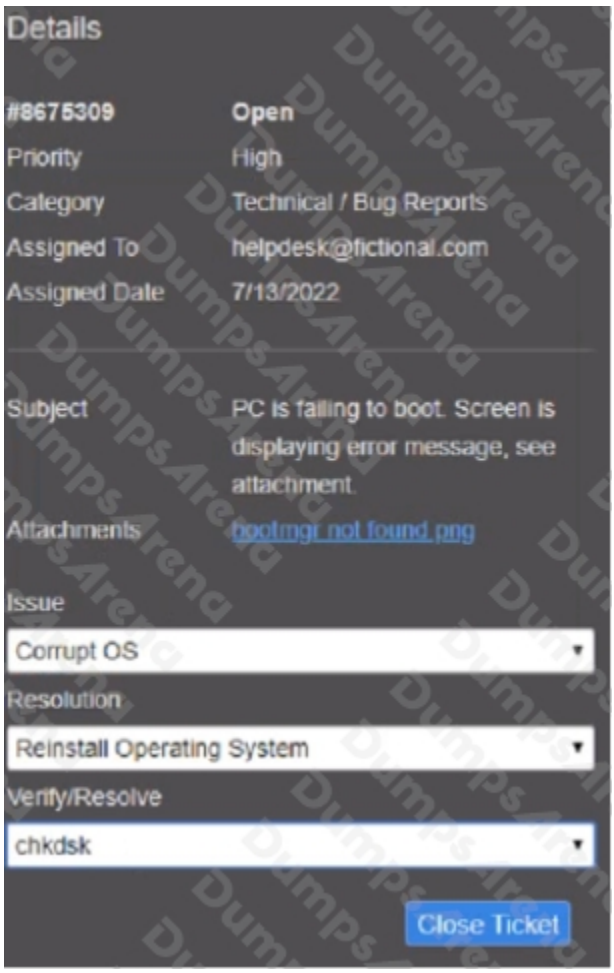

Details
Date
Priority
ing to boot. Screen i...
7/13/2022
Hi
access Z: on my co...
7/13/2022
Low
#8675309
Open
Priority
High
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
7/13/2022
Subject
PC is failing to boot. Screen is displaying error message, see attachment
Attachments
bootmgr not found.png
Issue
Resolution
Verify/Resolve


Details
Date
Priority
#8675309
Open
Priority
High
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
7/13/2022
Subject
PC is failing to boot. Screen is displaying error message, see attachment.
Attachments
bootmgr not found.jpg
Issue
Corrupt OS
Recent Windows Updates
Graphics Drive Updates
BSOD
Printing Issues
Limited Network Connectivity
Services Failed to Start
User Profile is Corrupted
Application Crash
User cannot access shared resource
URL contains typo
Resolution
Reinstall Operating System
Rollback Updates
Rollback Drivers
Repair Application
Restart Print Spooler
Disable Network Adapter
Update Network Drivers
Refresh DHCP
Rebuild Windows Profile
Apply Updates
Repair Installation
Restore from Recovery Partition
Remap network drive
Verify integrity of disk drive
Initiate screen share session with user
Windows recovery environment
Inform user of AUP violation
Verify/Resolve
chkdsk
dism
diskpart
sfc
dd
ctrl + alt + del
net use
net user
netstat
netsh
bootrec

ANSWER:


Details
Date
Priority
#8675309
Open
Priority
High
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
7/13/2022
Subject
PC is failing to boot. Screen is displaying error message, see attachment
Attachments
Issue
Corrupt OS
Recent Windows Updates
Graphics Drive Updates
BSOD
Printing Issues
Limited Network Connectivity
Services Failed to Start
User Profile is Corrupted
Application Crash
User cannot access shared resource
URL contains typo
Resolution
Reinstall Operating System
Rollback Updates
Rollback Drivers
Repair Application
Restart Print Spooler
Disable Network Adapter
Update Network Drivers
Refresh DHCP
Rebuild Windows Profile
Apply Updates
Repair installation
Restore from Recovery Partition
Remap network drive
Verify integrity of disk drive
Initiate screen share session with user
Windows recovery environment
Inform user of AUP violation
Verify/Resolve
chkdsk
dism
diskpart
sfc
dd
ctrl + alt + del
net use
net user

Explanation:



QUESTION NO: 10

In which of the following scenarios would remote wipe capabilities MOST likely be used? (Select TWO).

A. A new IT policy requires users to set up a lock screen PIN.

B. A user is overseas and wants to use a compatible international SIM Card.

C. A user left the phone at home and wants to prevent children from gaining access to the phone.

D. A user traded in the company phone for a cell carrier upgrade by mistake.

E. A user cannot locate the phone after attending a play at a theater.
A user cannot locate the phone after attending a play at a theater. F. A user forgot the phone in a taxi, and the driver called the company to return the device1
In scenario E, remote wipe capabilities would be used to prevent unauthorized access to the device and to protect sensitive data. In scenario F, remote wipe capabilities would be used to erase all data on the device before it is returned to the user.

F. A user forgot the phone in a taxi, and the driver called the company to return the device.

ANSWER: E F

Explanation:

Remote wipe capabilities are used to erase all data on a mobile device remotely. This can be useful in situations where a device is lost or stolen, or when sensitive data needs to be removed from a device. Remote wipe capabilities are most likely to be used in the following scenarios:

E. A user cannot locate the phone after attending a play at a theater. F. A user forgot the phone in a taxi, and the driver called the company to return the device1

In scenario E, remote wipe capabilities would be used to prevent unauthorized access to the device and to protect sensitive data. In scenario F, remote wipe capabilities would be used to erase all data on the device before it is returned to the user.

QUESTION NO: 11

A user reports a PC is running slowly. The technician suspects high disk I/O. Which of the following should the technician perform NEXT?

A. resmon_exe

B. dfrgui_exe

C. msinf032exe

D. msconfig_exe

ANSWER: A

Explanation:

If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O1. Resource Monitor provides detailed information about the system's resource usage, including disk I/O1. The technician can use this information to identify the process that is causing the high disk I/O and take appropriate action1.

QUESTION NO: 12

Which of the following file extensions are commonly used to install applications on a macOS machine? (Select THREE).

A. .mac

B. .Pkg

C. .deb

D. .dmg

E. .msi

F. .appx

G. .app

H. .apk

ANSWER: B D G

Explanation:

https://support.microsoft.com/en-us/windows/common-file-name-extensions-in-windows-da4a4430-8e76-89c5-59f7-1cdbbc75cb01

.pkg and .dmg are files used to distribute and install applications on macOS. .pkg files are installer packages that may contain multiple files and executable code, while .dmg files are disk images that can contain a single bundled application or multiple applications. .app files are typically the main executable files for macOS applications. The other options listed are file extensions for applications or installers on other platforms (such as .deb for Debian-based Linux systems, .msi for Windows, and .apk for Android). This information is covered in the Comptia A+ Core2 documents/guide under the Mac OS section.

QUESTION NO: 13

A field technician applied a Group Policy setting to all the workstations in the network. This setting forced the workstations to use a specific SNTP server. Users are unable to log in now. Which of the following is the MOST likely cause of this issue?

A. The SNTP server is offline.

B. A user changed the time zone on a local machine.

C. The Group Policy setting has disrupted domain authentication on the system,

D. The workstations and the authentication server have a system clock difference.

ANSWER: D

Explanation:

The workstations and the authentication server have a system clock difference. If a Group Policy setting is applied that forces the workstations to use a specific SNTP server, but the system clock on the workstations and the authentication server are out of sync, then this can cause authentication issues and users will be unable to log in. In this case, the most likely cause of the issue is a difference in system clocks and the technician should ensure that the clocks on the workstations and the authentication server are in sync.

QUESTION NO: 14

A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

A. Scan the computer with the company-provided antivirus software

B. Install a new hard drive and clone the user's drive to it

C. Deploy an ad-blocking extension to the browser.

D. Uninstall the company-provided antivirus software

E. Click the link in the messages to pay for virus removal

F. Perform a reset on the user's web browser

ANSWER: C F

Explanation:

"The user thought the company-provided antivirus software would prevent this issue."

The most likely steps to resolve the issue are to deploy an ad-blocking extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or settings that may be causing the issue.

QUESTION NO: 15

Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

A. Multifactor authentication

B. Badge reader

C. Personal identification number

D. Firewall

E. Motion sensor

F. Soft token

ANSWER: B E

Explanation:

Badge reader and motion sensor are devices that can be deployed to enhance physical security for a building. A badge reader is a device that scans and verifies an identification card or tag that grants access to authorized personnel only. A badge reader can help prevent unauthorized entry or intrusion into a building or a restricted area. A motion sensor is a device that detects movement and triggers an alarm or an action when motion is detected. A motion sensor can help deter or alert potential intruders or trespassers in a building or an area. Multifactor authentication is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. Multifactor authentication is not a device that can be deployed to enhance physical security for a building but a technique that can be

used to enhance logical security for systems or services. Personal identification number is a numeric code that can be used as part of authentication or access control. Personal identification number is not a device that can be deployed to enhance physical security for a building but an example of something you know factor in multifactor authentication. Firewall is a device or software that filters network traffic based on rules and policies. Firewall is not a device that can be deployed to enhance physical security for a building but a device that can be used to enhance network security for systems or services. Soft token is an application or software that generates one-time passwords or codes for authentication purposes. Soft token is not a device that can be deployed to enhance physical security for a building but an example of something you have factor in multifactor authentication. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3