DUMPSARENA

CompTIA A+ Certification Core 2 Exam

CompTIA 220-1102

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 technician is setting up a conference room computer with a script that boots the application on login. Which of the following would the technician use to accomplish this task? (Select TWO).

A. File Explorer

B. Startup Folder

C. System Information

D. Programs and Features

E. Task Scheduler

F. Device Manager

ANSWER: B E

QUESTION NO: 2

A technician installed a known-good, compatible motherboard on a new laptop. However, the motherboard is not working on the laptop. Which of the following should the technician MOST likely have done to prevent damage?

A. Removed all jewelry

B. Completed an inventory of tools before use

C. Practiced electrical fire safety

D. Connected a proper ESD strap

ANSWER: A

Explanation:

The technician should have connected a proper ESD strap to prevent damage to the motherboard. ESD (electrostatic discharge) can cause damage to electronic components, and an ESD strap helps to prevent this by grounding the technician and preventing the buildup of static electricity. Removing all jewelry is also a good practice, but it is not the most likely solution to this problem.

QUESTION NO: 3

Which of the following only has a web browser interface?

A. Linux

B. Microsoft Windows

C. iOS

D. Chromium

ANSWER: D

Explanation:

Chromium is an operating system that only has a web browser interface. Chromium is an open-source project that provides the source code and framework for Chrome OS, which is a Linux-based operating system developed by Google. Chromium and Chrome OS are designed to run web applications and cloud services through the Chrome web browser, which is the only user interface available on the system. Chromium and Chrome OS are mainly used on devices such as Chromebooks, Chromeboxes and Chromebits. Linux is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Linux is an open-source and customizable operating system that can run various applications and services on different devices and platforms. Linux can also support different web browsers, such as Firefox, Opera and Chromium. Microsoft Windows is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Microsoft Windows is a proprietary and popular operating system that can run various applications and services on different devices and platforms. Microsoft Windows can also support different web browsers, such as Edge, Internet Explorer and Chrome. iOS is an operating system that does not only have a web browser interface but also a graphical user interface and a voice-based interface. iOS is a proprietary and mobile operating system developed by Apple that can run various applications and services on devices such as iPhone, iPad and iPod Touch. iOS can also support different web browsers, such as Safari, Firefox and Chrome. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

QUESTION NO: 4

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: 5

A technician is working to resolve a Wi-Fi network issue at a doctor's office that is located next to an apartment complex. The technician discovers that employees and patients are not the only people on the network. Which of the following should the technician do to BEST minimize this issue?

A. Disable unused ports.

B. Remove the guest network

C. Add a password to the guest network

D. Change the network channel.

ANSWER: D

Explanation:

Changing the network channel is the best solution to minimize the issue of employees and patients not being the only people on the Wi-Fi network5

References: 3. Sample CompTIA Security+ exam questions and answers. Retrieved from https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-Security-exam-questions-and-answers

QUESTION NO: 6 - (SIMULATION)

A user reports that after a recent software deployment to upgrade applications, the user can no longer use the Testing program.

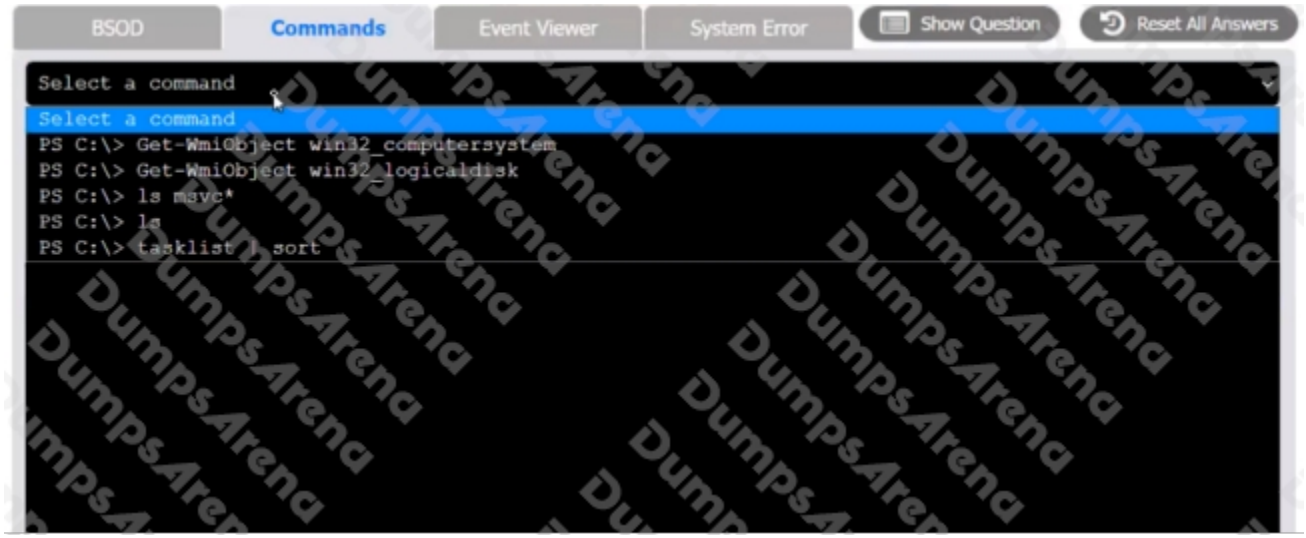
However, other employees can successfully use the Testing program.

INSTRUCTIONS

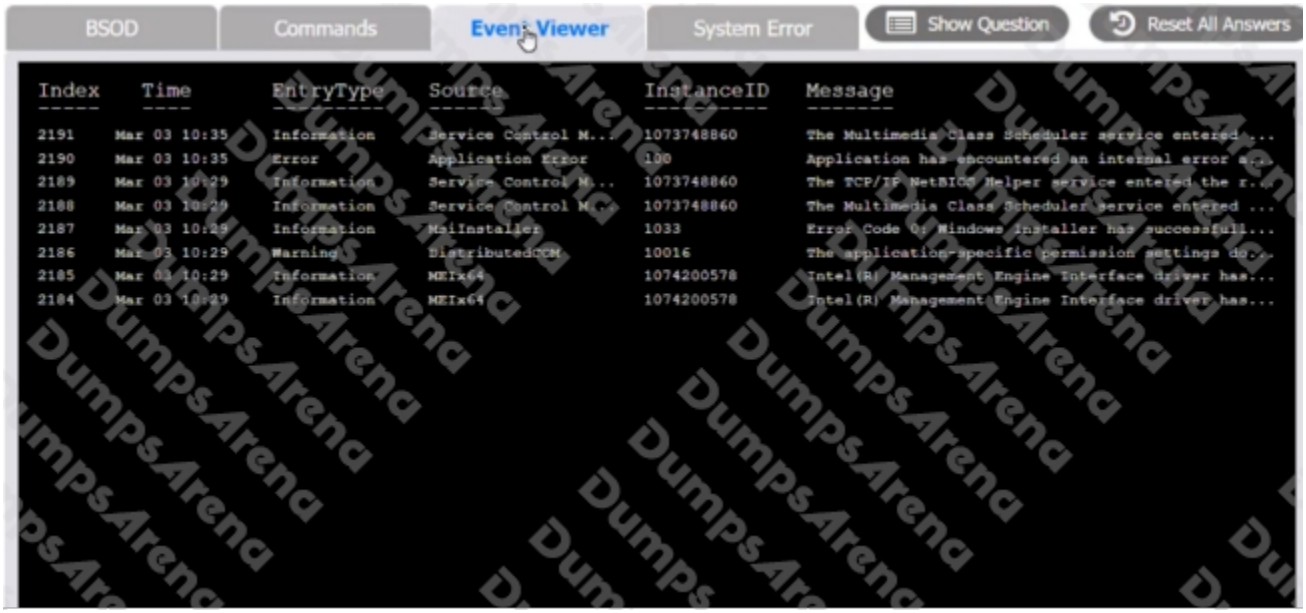
Review the information in each tab to verify the results of the deployment and resolve any issues discovered by selecting the:

BSOD

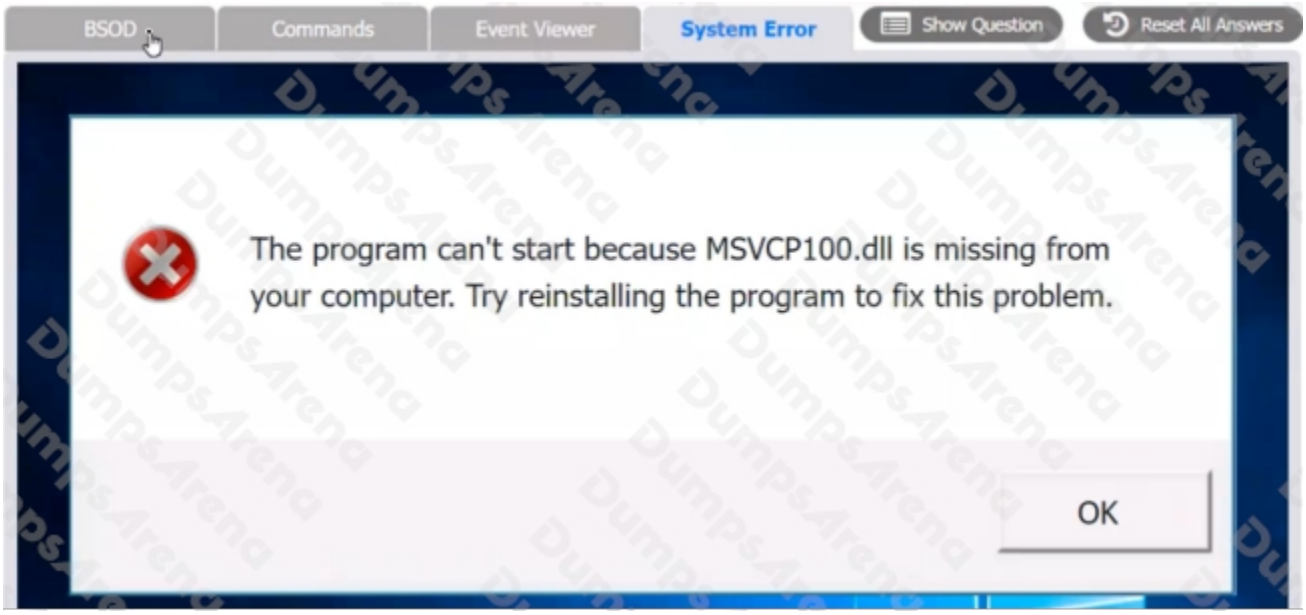
Commands:



Event Viewer:



System Error:



ANSWER: Pending

QUESTION NO: 7

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: 8

A technician is asked to resize a partition on the internal storage drive of a computer running macOS. Which of the followings tools should the technician use to accomplish this task?

A. Consoltf

B. Disk Utility

C. Time Machine

D. FileVault

ANSWER: B

Explanation:

The technician should use Disk Utility to resize a partition on the internal storage drive of a computer running macOS. Disk Utility is a built-in utility that allows users to manage disks, partitions, and volumes on a Mac. It can be used to resize, create, and delete partitions, as well as to format disks and volumes.

QUESTION NO: 9

An organization implemented a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. Which of the following wireless security methods BEST describes what this organization implemented?

A. TKIP

B. RADIUS

C. WPA2

D. AES

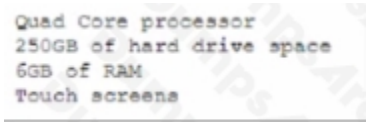
ANSWER: B

Explanation:

RADIUS stands for Remote Authentication Dial-In User Service and it is a protocol that provides centralized authentication, authorization, and accounting for network access. RADIUS can be used to implement a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. This is also known as 802.1X authentication or EAP-TLS authentication

QUESTION NO: 10

A department has the following technical requirements for a new application:



The company plans to upgrade from a 32-bit Windows OS to a 64-bit OS. Which of the following will the company be able to fully take advantage of after the upgrade?

A. CPU

B. Hard drive

C. RAM

D. Touch screen

ANSWER: C

Explanation:

https://www.makeuseof.com/tag/difference-32-bit-64-bit-windows/

After upgrading from a 32-bit Windows OS to a 64-bit OS, the company will be able to fully take advantage of the RAM of the computer. This is because a 64-bit operating system is able to use larger amounts of RAM compared to a 32-bit operating system, which may benefit the system's overall performance if it has more than 4GB of RAM installed

QUESTION NO: 11

An implementation specialist is replacing a legacy system at a vendor site that has only one wireless network available. When the specialist connects to Wi-Fi. the specialist realizes the insecure network has open authentication. The technician needs to secure the vendor's sensitive data. Which of the following should the specialist do FIRST to protect the company's data?

A. Manually configure an IP address, a subnet mask, and a default gateway.

B. Connect to the vendor's network using a VPN.

C. Change the network location to private.

D. Configure MFA on the network.

ANSWER: B

Explanation:

The first thing that the specialist should do to protect the company's data on an insecure network with open authentication is to connect to the vendor's network using a VPN. A VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public or untrusted network. A VPN can protect the company's data by preventing eavesdropping, interception or modification of the network traffic by unauthorized parties. A VPN can also provide access to the company's internal network and resources remotely. Manually configuring an IP address, a subnet mask and a default gateway may not be necessary or possible if the vendor's network uses DHCP to assign network configuration parameters automatically. Manually configuring an IP address, a subnet mask and a default gateway does not protect the company's data from network attacks or threats. Changing the network location to private may not be advisable or effective if the vendor's network is a public or untrusted network. Changing the network location to private does not protect the company's data from network attacks or threats. Configuring MFA on the network may not be feasible or sufficient if the vendor's network has open authentication and does not support or require MFA. Configuring MFA on the network does not protect the company's data from network attacks or threats. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

QUESTION NO: 12

A desktop engineer is deploying a master image. Which of the following should the desktop engineer consider when building the master image? (Select TWO).

A. Device drivers

B. Keyboard backlight settings

C. Installed application license keys

D. Display orientation

E. Target device power supply

F. Disabling express charging

ANSWER: A C

QUESTION NO: 13

A possible cause of the user being redirected to unexpected websites is that the localhost file entries have been modified by malware or hackers to point to malicious or unwanted websites. The localhost file is a text file that maps hostnames to IP addresses and can override DNS settings. By examining the localhost file entries, a technician can identify and remove any suspicious or unauthorized entries that may cause the redirection issue. Enabling firewall ACLs may not resolve the issue if the firewall rules do not block the malicious or unwanted websites. Verifying the routing tables may not resolve the issue if the routing configuration is correct and does not affect the web traffic. Updating the antivirus definitions may help prevent future infections but may not remove the existing malware or changes to the localhost file. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3a

A network technician installed a SOHO router for a home office user. The user has read reports about home routers being targeted by malicious actors and then used in DDoS attacks. Which of the following can the technician MOST likely do to defend against this threat?

A. Add network content filtering.

B. Disable the SSID broadcast.

C. Configure port forwarding.

D. Change the default credentials.

ANSWER: D

Explanation:

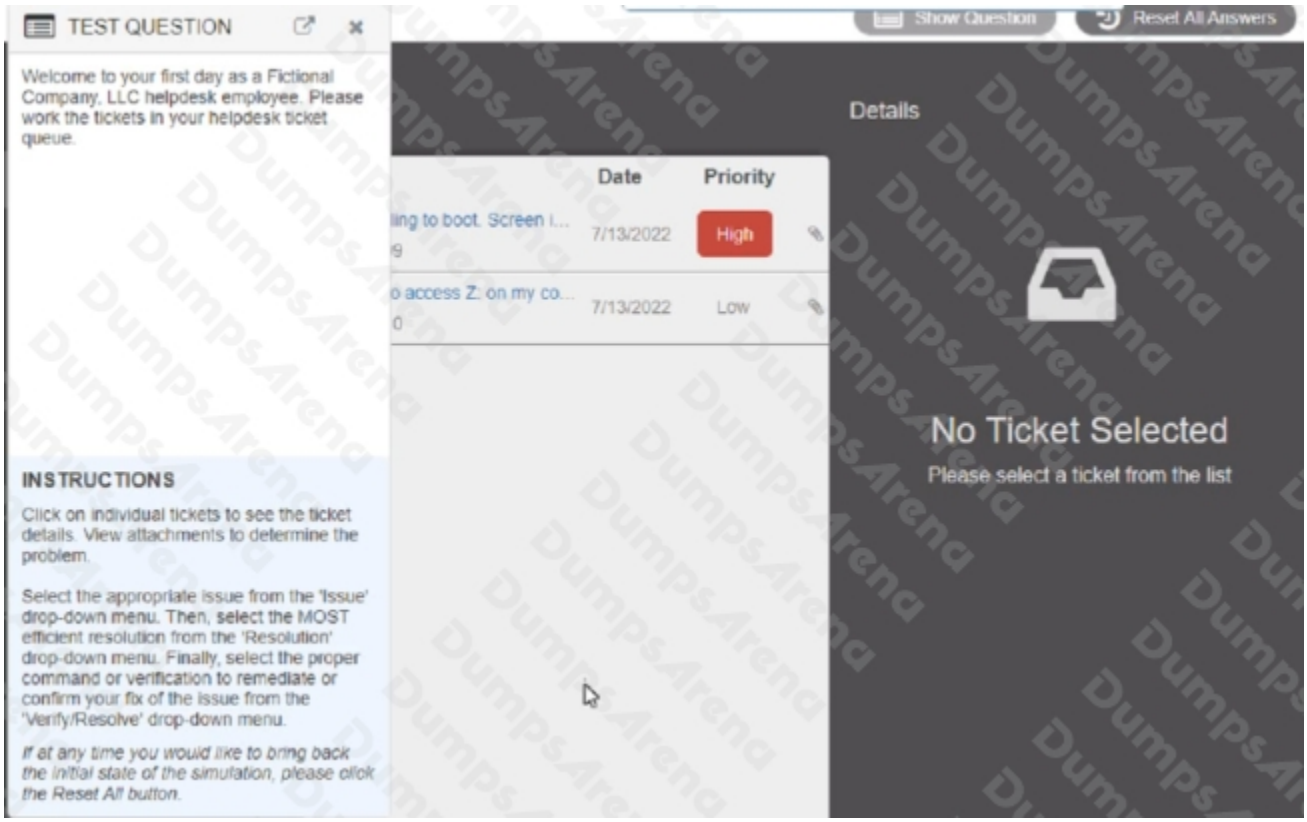
One of the most effective ways to defend against malicious actors targeting home routers for DDoS attacks is to change the default credentials of the router. The default credentials are often well-known or easily guessed by attackers, who can then access and compromise the router settings and firmware. By changing the default credentials to strong and unique ones, a technician can prevent unauthorized access and configuration changes to the router. Adding network content filtering may help block some malicious or unwanted websites but may not prevent attackers from exploiting router vulnerabilities or backdoors. Disabling the SSID broadcast may help reduce the visibility of the wireless network but may not prevent attackers from scanning or detecting it. Configuring port forwarding may help direct incoming traffic to specific devices or services but may not prevent attackers from sending malicious packets or requests to the router. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

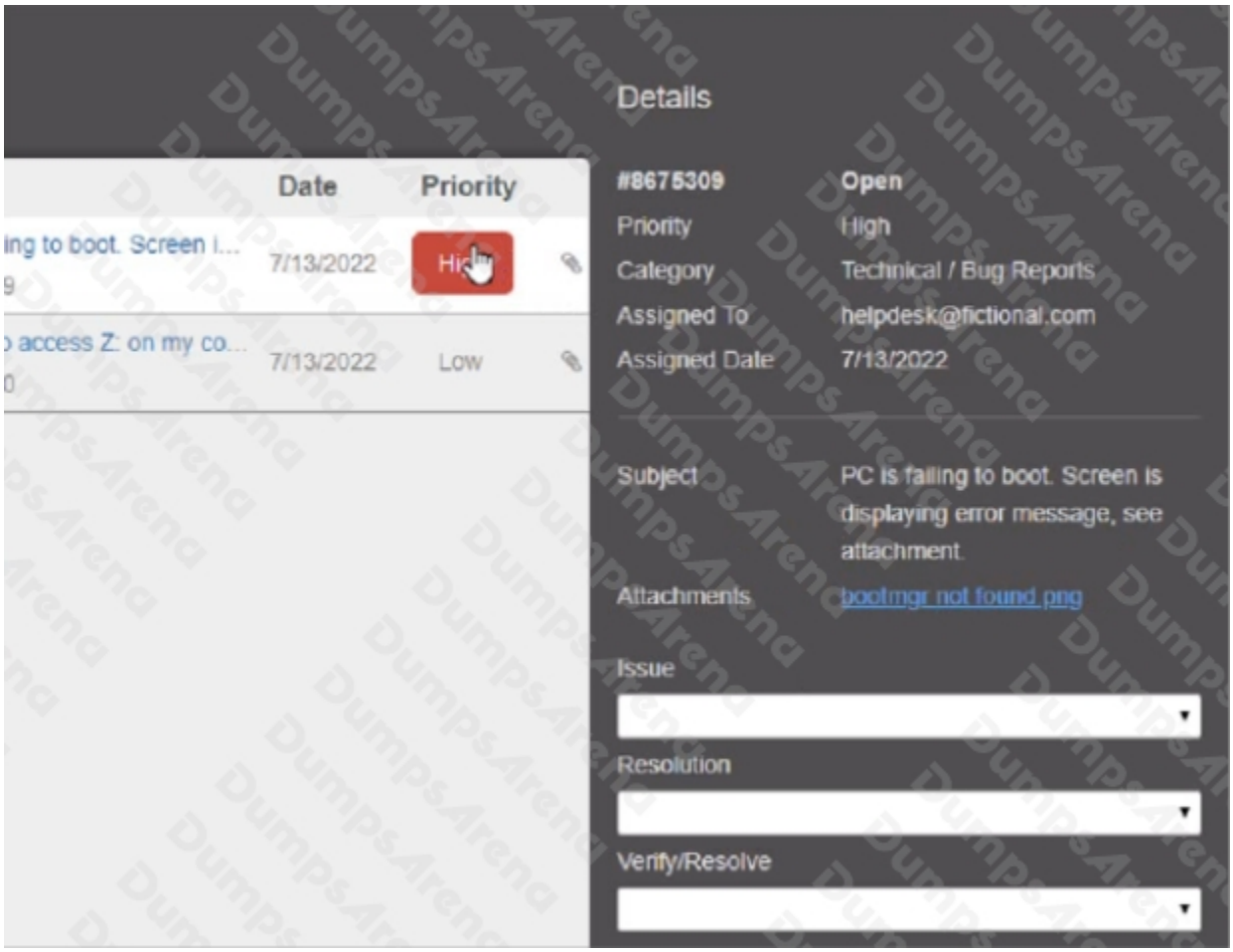
QUESTION NO: 14 - (HOTSPOT)

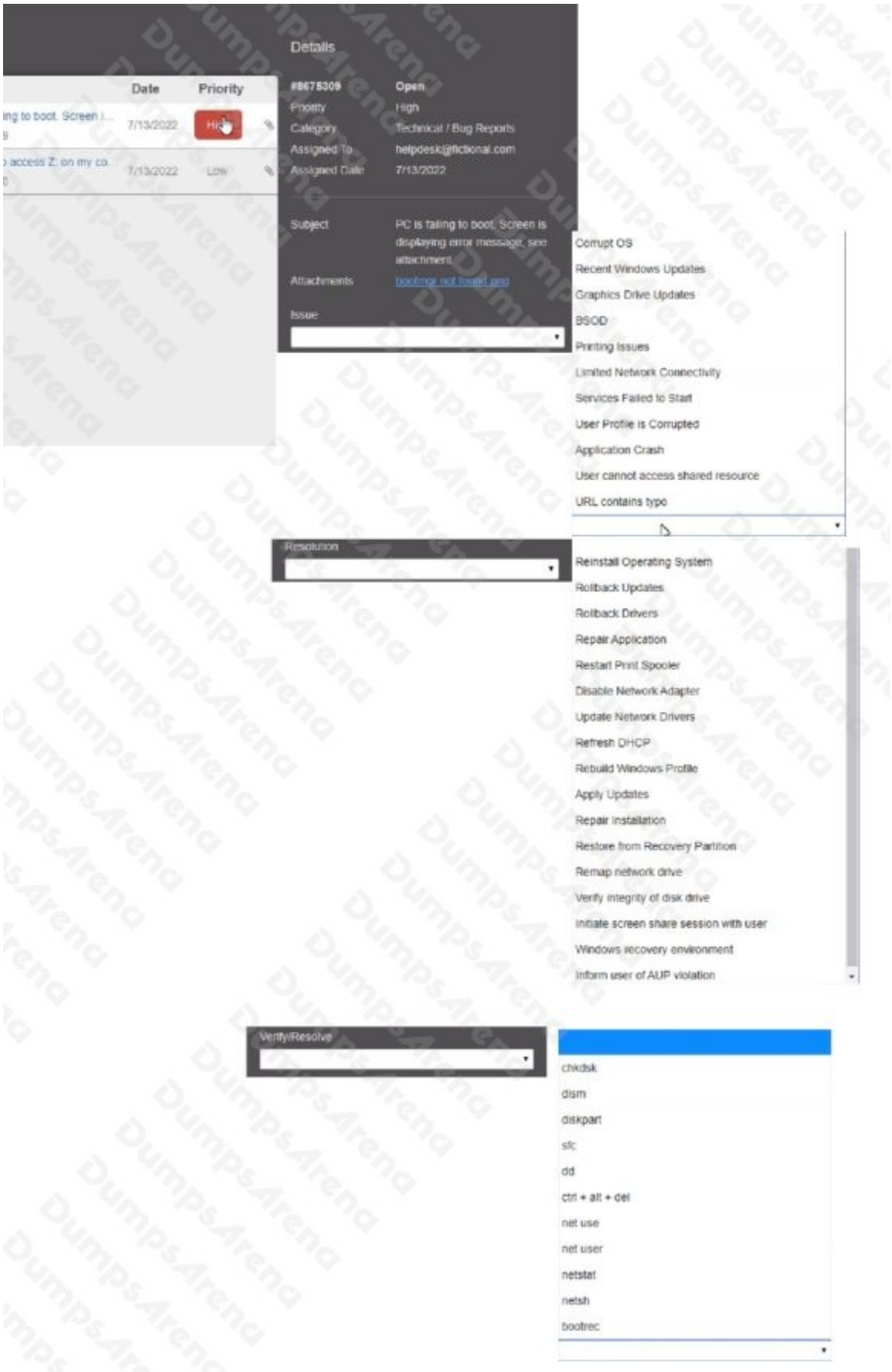
Welcome to your first day as a Fictional Company. LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

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.

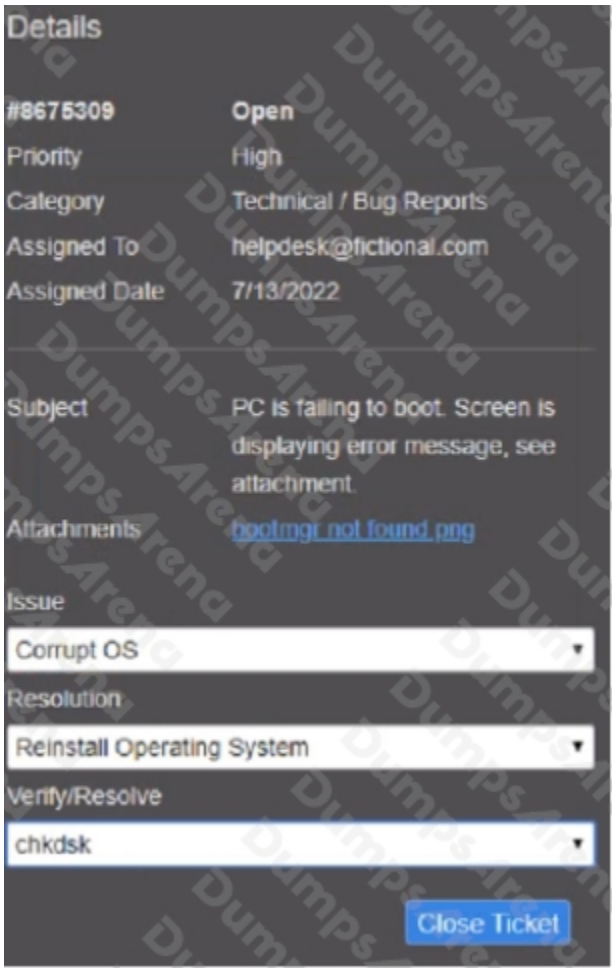

TEST QUESTION
Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.
INSTRUCTIONS
Click on individual tickets to see the ticket details. View attachments to determine the problem.
Select the appropriate issue from the 'Issue' drop-down 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:

Explanation:



QUESTION NO: 15

A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

A. Utilizing an ESD strap

B. Disconnecting the computer from the power source

C. Placing the PSU in an antistatic bag

D. Ensuring proper ventilation

E. Removing dust from the ventilation fans

F. Ensuring equipment is grounded

ANSWER: A C

Explanation:

The two safety procedures that would best protect the components in the PC are:

https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/

https://www.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158