- **Vendor: CompTIA**
- **Exam Code: 220-1002**
- **Exam Name: CompTIA A+ Certification Exam: Core 2**
- **New Updated Questions from Braindump2go (Updated in Feb./2021)**

QUESTION 526
Following instructions from the help desk, a company employee turns off a workstation that has a suspected ransomware infection. A technician is dispatched later to investigate the workstation. Which of the following should the technician perform FIRST?

A. Disconnect the network cable.
B. Disable System Restore
C. Boot into safe mode
D. Update the antivirus software.
E. Recover from a restore point

Answer: A

QUESTION 527
Which of the following has the ability to allow or deny POP3 traffic on the firewall?

A. Email filtering
B. MAC filtering
C. Port security
D. Access control list

Answer: D

QUESTION 528
A technician configures a switch for an enterprise to use 802.1X.
Which of the following logical security concepts uses 802.1X?

A. Access control list
B. MAC address filtering
C. MDM policies
D. Port security

Answer: A

QUESTION 529
A technician deployed a new file server on the network. The technician wants to map the file server as a network drive on all users' computers when they log onto the network by creating a logon script. Which of the following should the technician use?

A. net use
B. dism
C. diskpart
D. gpresult

Answer: B

QUESTION 530
Ann, an employee, recently reported to the company's IT technician that her smartphone is exhibiting strange behavior. When she opens the application store. an error appears that indicates there is no connection. However, the phone still receives emails and can access the Internet from the browser. The phone was backed up recently and auto-connects to a VPN. Which of the following troubleshooting steps should the technician take NEXT? (Select TWO)

A. Reset the network settings
B. Uninstall the application store.
C. Restore from a backup.
D. Clear the application cache and data
E. Check the time and date settings.
F. Reset application preferences.

Answer: AE

QUESTION 531
A technician was alerted by IT security of a potentially infected desktop, which is at a remote location. The technician will arrive on site after one hour. Which of the following steps should be performed prior to traveling to prevent further infection? (Select TWO).

A. Start syst m updates.
B. Backup PC data
C. Run antivirus
D. Install the firewall.
E. Turn off System Restore
F. Install a keylogger

Answer: CD

QUESTION 532
A remote user has reported a suspicious pop-up, and a technician is troubleshooting the user's laptop. The technician needs to connect securely to the computer to view the user's screen and investigate the issue. Which of the following should the technician use?

A. SSH
B. MSTSC
C. SFTP
D. MSRA

Answer: D

QUESTION 533
The Chief Executive Officer (CEO) of an organization frequently travels with sensitive data on a laptop and is concerned the data could be compromised if the laptop is lost or stolen.
Which of the following should the technician recommend to BEST ensure the data is not compromised if the laptop is lost or stolen?

A. Implement strong password policies.

B. Encrypt the hard drive on the laptop.
C. Set up a BIOS password on the laptop.
D. Enable multifactor authentication on the laptop.

Answer: B

QUESTION 534
A technician is decommissioning a workstation that contains Pll The HDDs cannot be used in another device, and all data must be destroyed.
Which of the following actions would BEST fulfill these requirements? (Select TWO)

A. Physically damage the drives.
B. Leave the drives in the workstation since it will be decommissioned
C. Take a picture of the drives individually and their serial numbers
D. Send the drive to a certified third-party vendor for destruction.
E. Perform a ow level format before removal
F. Set a complex hard drive password.

Answer: AD

QUESTION 535
To which of the following should a technician ground an ESD strap when adding memory to a workstation?

A. Computer chassis
B. Surge protector
C. Wooden workbench
D. Power supply

Answer: A

QUESTION 536
A technician recently built a gaming PC with a multicode CPU, 32GB DDR4 memory, a 1TB SSD. and a high-end GPU. The technician installed the OS and a new game but noticed the frame-rate performance was much lower than expected.
Which of the following should the technician do NEXT to address the performance issues?

A. Install a higher wattage PSU.
B. Download security patches
C. Defragment the drive
D. Update the device drivers

Answer: D

QUESTION 537
A technician is troubleshooting vendor-specific software. Which of the following is where the technician should go to find problem-specific fixes on the vendor's website?

A. Software user manual
B. Knowledge base articles
C. System requirements documentation
D. Installation instructions

Answer: B

QUESTION 538

A customer recently upgraded from Windows 7 to Windows 10. The customer lost access to certain network shares, and the system keeps preventing the user's access. Which of the following is the MOST likely cause of the issue?

A. The BitLocker feature was activated and encrypted the shares.
B. The user's information was not preserved during the upgrade
C. Windows Firewall no longer allows access to legacy systems.
D. The network login script executed incorrectly.

Answer: D

QUESTION 539
A recent security breach has caused a large company to audit its own internal security policy. The breach Involved an unauthorized user gaming access to an unattended computer by exploiting default credentials and then further elevating system privileges. Which of the following security measures would have MOST likely prevented the breach? (Select TWO).

A. Account lockout policy
B. Disabled guest account
C. Screensaver password locks
D. BIOS password
E. Password expiration
F. Logon time restrictions

Answer: BC

QUESTION 540
Which of the following employs content filtering to prevent data leaks within an organization?

A. DLP
B. IPS
C. ACL
D. VPN

Answer: A

QUESTION 541
Which of the following Windows technologies can render a Me unreadable by anyone other than the file's creator?

A. EFS
B. DFS
C. Bit Locker
D. NTFS

Answer: D