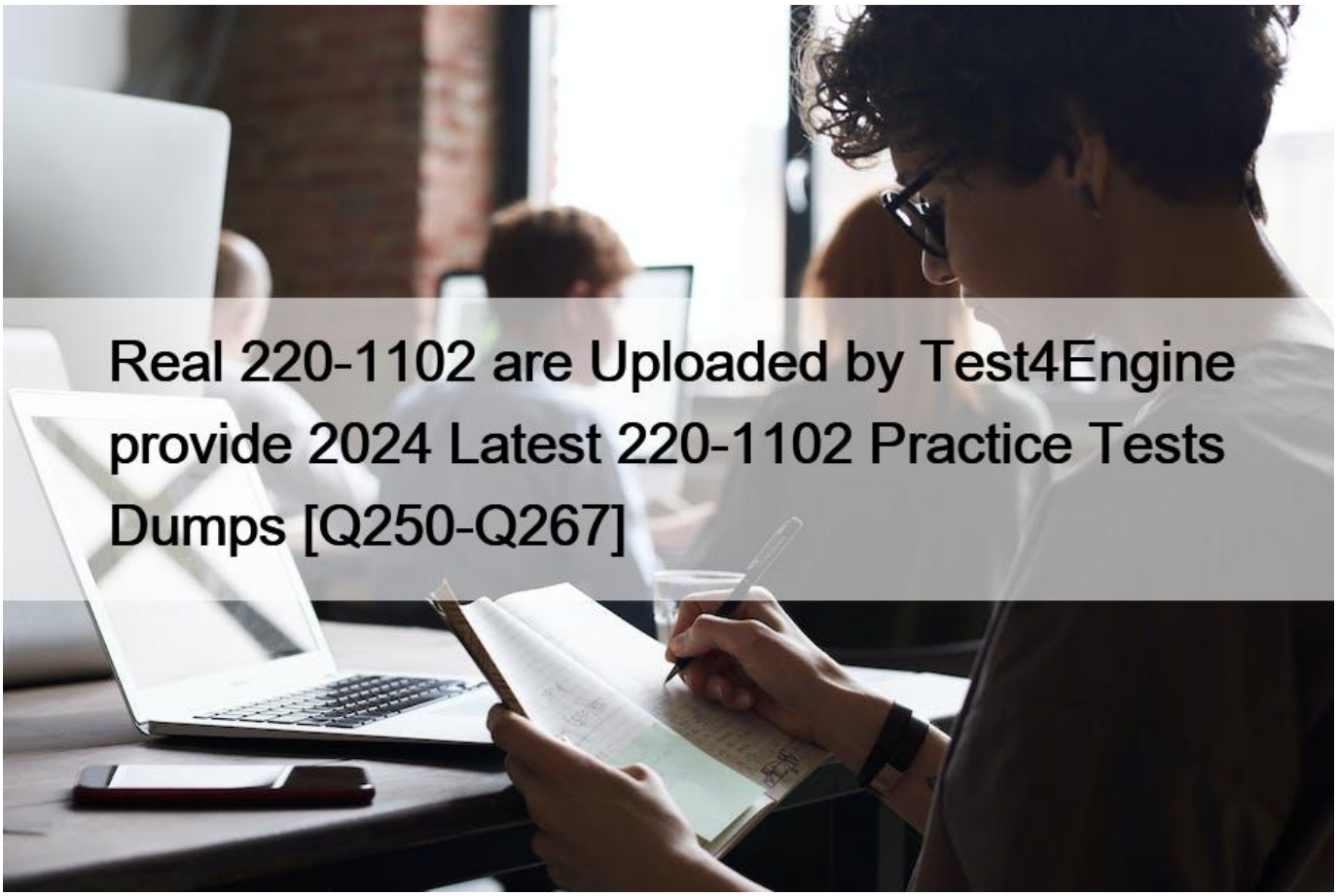
Real 220-1102 are Uploaded by Test4Engine provide 2024 Latest 220-1102 Practice Tests Dumps [Q250-Q267



Real 220-1102 are Uploaded by **Test4Engine** provide **2024** Latest 220-1102 Practice Tests Dumps.
All 220-1102 Dumps and CompTIA A+ Certification Exam: Core 2 Training Courses Help candidates to study and pass the CompTIA A+ Certification Exam: Core 2 Exams hassle-free! QUESTION 250

Which of the following file extensions are commonly used to install applications on a macOS machine?

(Select THREE).
* .mac
* .Pkg
* .deb
* .dmg
* .msi
* .appx
* .app
* .apk

https://support.microsoft.com/en-us/windows/common-file-name-extensions-in-windows-da4a4430-8e76-89c5-5

.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 251

A company would like to implement multifactor authentication for all employees at a minimal cost. Which of the following best meets the company’s requirements?
* Biometrics
* Soft token
* Access control lists
* Smart card
Explanation

A soft token, also known as a software token or an OTP (one-time password) app, is a type of multifactor authentication that generates a temporary code or password on a user’s device, such as a smartphone or a tablet. The user must enter this code or password along with their username and password to access their account or service. A soft token can help improve security by adding an extra layer of verification and preventing unauthorized access even if the user’s credentials are compromised. A soft token can also be implemented at a minimal cost, as it does not require any additional hardware or infrastructure. Biometrics, access control lists, and smart card are not types of multifactor authentication that can be implemented at a minimal cost.

QUESTION 252

A technician is moving a Windows workstation from the accounting department to the sales department and needs to update the IP and gateway settings. Which of the following Control Panel utilities should the technician use?
* Programs and Features
* Network and Sharing Center
* User Accounts
* Device Manager
The Network and Sharing Center is a Control Panel utility that allows users to view and modify network settings, such as IP address, subnet mask, default gateway, DNS servers, and network profiles. To change the IP and gateway settings of a Windows workstation, the technician can follow these steps:

* Open the Network and Sharing Center by clicking on the network icon in the system tray or by searching for it in the Start menu.

* Click on Change adapter settings on the left sidebar.

* Right-click on the network adapter that is connected to the network and select Properties.

* Double-click on Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6) depending on the network protocol used.

* Select Use the following IP address and enter the desired IP address, subnet mask, and default gateway for the workstation. Alternatively, select Obtain an IP address automatically if the network uses DHCP to assign IP addresses dynamically.

* Click OK to save the changes and close the dialog boxes.

References:

* The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2171

* How to change the IP address in Windows 10 and Windows 11 (4 ways), section 12

QUESTION 253

A systems administrator is monitoring an unusual amount of network traffic from a kiosk machine and needs to Investigate to determine the source of the traffic. Which of the following tools can the administrator use to view which processes on the kiosk machine are connecting to the internet?
* Resource Monitor
* Performance Monitor
* Command Prompt
* System Information
Explanation

Resource Monitor is a tool that shows the network activity of each process on a Windows machine, including the TCP connections and the sent and received bytes. Performance Monitor is a tool that shows the performance metrics of the system, such as CPU, memory, disk and network usage. Command Prompt is a tool that allows running commands and scripts on a Windows machine. System Information is a tool that shows the hardware and software configuration of a Windows machine. Verified References:

https://www.comptia.org/blog/how-to-use-resource-monitor https://www.comptia.org/certifications/a

QUESTION 254

A user calls the help desk to report potential malware on a computer. The anomalous activity began after the user clicked a link to a free gift card in a recent email The technician asks the user to describe any unusual activity, such as slow performance, excessive pop-ups, and browser redirections. Which of the following should the technician do NEXT?
* Advise the user to run a complete system scan using the OS anti-malware application
* Guide the user to reboot the machine into safe mode and verify whether the anomalous activities are still present
* Have the user check for recently installed applications and outline those installed since the link in the email was clicked
* Instruct the user to disconnect the Ethernet connection to the corporate network.
Explanation

First thing you want to do is quarantine/disconnect the affected system from the network so whatever malicious software doesn’t spread.

QUESTION 255

A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Select TWO).
* File Explorer
* User Account Control
* Windows Backup and Restore
* Windows Firewall
* Windows Defender
* Network Packet Analyzer
The correct answers are E. Windows Defender and A. File Explorer. Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorer can be used to locate and delete files associated with the malicious software1

QUESTION 256

A technician receives an invalid certificate error when visiting a website. Other workstations on the same local network are unable to replicate this issue. Which of the following is most likely causing the issue?
* Date and time
* User access control
* UEFI boot mode
* Log-on times

Date and time is the most likely cause of the issue. The date and time settings on a workstation affect the validity of the certificates used by websites to establish secure connections. If the date and time are incorrect, the workstation may not recognize the certificate as valid and display an invalid certificate error. Other workstations on the same local network may not have this issue if their date and time are correct. User access control, UEFI boot mode, and log-on times are not likely causes of the issue. User access control is a feature that prevents unauthorized changes to the system by prompting for confirmation or credentials. UEFI boot mode is a firmware interface that controls the boot process of the workstation. Log-on times are settings that restrict when a user can log in to the workstation. None of these factors affect the validity of the certificates used by websites. Reference:

Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14 CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 456

QUESTION 257

A user reports a virus is on a PC. The user installs additional real-lime protection antivirus software, and the PC begins performing extremely slow. Which of the following steps should the technician take to resolve the issue?
* Uninstall one antivirus software program and install a different one.
* Launch Windows Update, and then download and install OS updates
* Activate real-time protection on both antivirus software programs
* Enable the quarantine feature on both antivirus software programs.
* Remove the user-installed antivirus software program.

Explanation

Removing the user-installed antivirus software program is the best way to resolve the issue of extremely slow performance caused by installing additional real-time protection antivirus software on a PC. Having more than one antivirus software program running at the same time can cause conflicts, resource consumption and performance degradation. Uninstalling one antivirus software program and installing a different one, activating real-time protection on both antivirus software programs, enabling the quarantine feature on both antivirus software programs and launching Windows Update are not effective ways to resolve the issue. Verified References:

https://www.comptia.org/blog/why-you-shouldnt-run-multiple-antivirus-programs-at-the-same-time

https://www.comptia.org/certifications/a

QUESTION 258

A company is experiencing a DDoS attack. Several internal workstations are the source of the traffic. Which of the following types of infections are the workstations most likely experiencing? (Select two).
* Zombies
* Keylogger
* Adware
* Botnet
* Ransomware

* Spyware

Explanation

Zombies and botnets are terms that describe the types of infections that can cause internal workstations to participate in a DDoS (distributed denial-of-service) attack. A DDoS attack is a malicious attempt to disrupt the normal functioning of a website or a network by overwhelming it with a large amount of traffic from multiple sources. Zombies are infected computers that are remotely controlled by hackers without the owners’ knowledge or consent. Botnets are networks of zombies that are coordinated by hackers to launch DDoS attacks or other malicious activities. Keylogger, adware, ransomware, and spyware are not types of infections that can cause internal workstations to participate in a DDoS attack.

QUESTION 259

A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities is the best choice for accessing the necessary configuration to complete this goal?

* Security and Maintenance
* Network and Sharing Center
* Windows Defender Firewall
* Internet Options

Explore

The correct answer is D. Internet Options. The Internet Options utility in Windows allows you to configure various settings related to your internet connection, including the proxy server settings. To access the Internet Options utility, you can either open the Control Panel and click on Internet Options, or open any web browser and click on the Tools menu and then on Internet Options. In the Internet Options window, go to the Connections tab and click on the LAN settings button. Here, you can enable or disable the use of a proxy server, as well as enter the address and port number of the proxy server you want to use12.

Security and Maintenance is a utility in Windows that allows you to view and manage the security and maintenance status of your computer, such as firewall, antivirus, backup, troubleshooting, and recovery settings. It does not have any option to configure proxy server settings.

Network and Sharing Center is a utility in Windows that allows you to view and manage your network connections, such as Wi-Fi, Ethernet, VPN, or dial-up. It also allows you to change network settings, such as network discovery, file and printer sharing, homegroup, and adapter settings. It does not have any option to configure proxy server settings.

Windows Defender Firewall is a utility in Windows that allows you to enable or disable the firewall protection for your computer, as well as configure firewall rules for inbound and outbound traffic. It does not have any option to configure proxy server settings.

QUESTION 260

A user’s iPhone was permanently locked after several tailed login attempts. Which of the following will restore access to the device?
* Fingerprint and pattern
* Facial recognition and PIN code
* Primary account and password
* Secondary account and recovery code

A secondary account and recovery code are used to reset the primary account and password on an iPhone after it has been locked due to failed login attempts. Fingerprint, pattern, facial recognition and PIN code are biometric or numeric methods that can be used to unlock an iPhone, but they are not helpful if the device has been permanently locked. Verified References:

https://support.apple.com/en-us/HT204306https://www.comptia.org/certifications/a

QUESTION 261

A technician is installing RAM in a new workstation and needs to protect against electrostatic discharge.

Which of the following will best resolve this concern?
* Battery backup
* Thermal paste
* ESD strap
* Consistent power

Explanation

An ESD strap, also known as an antistatic wrist strap, is a device that prevents electrostatic discharge (ESD) from damaging sensitive electronic components such as RAM. ESD is the sudden flow of electricity between two objects with different electrical charges, which can cause permanent damage or malfunction to electronic devices. An ESD strap connects the technician’s wrist to a grounded surface, such as a metal case or a mat, and equalizes the electrical potential between the technician and the device. Battery backup, thermal paste, and consistent power are not devices that can protect against ESD.

QUESTION 262

A user’s mobile phone has become sluggish A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).
* Prevent a device root
* Disable biometric authentication
* Require a PIN on the unlock screen
* Enable developer mode
* Block a third-party application installation
* Prevent GPS spoofing

Explanation

To help secure the device against this threat in the future, the administrator should require a PIN on the unlock screen and block a third-party application installation. Requiring a PIN on the unlock screen can help to prevent unauthorized access to the device, while blocking third-party application installation can help to prevent malicious applications from being installed on the device.

QUESTION 263

A user added a second monitor and wants to extend the display to it. In which of the following Windows settings will the user

MOST likely be able to make this change?
* System
* Devices
* Personalization
* Accessibility

Explanation

The user can most likely make the change of extending the display to a second monitor in the System option in the Windows settings. The System option allows users to manage system settings and features, such as display, sound, notifications, power and storage. The user can extend the display to a second monitor by selecting Display from the System option and then choosing Extend these displays from the Multiple displays drop-down menu. This will allow the user to use both monitors as one large desktop area. Devices is an option in the Windows settings that allows users to add and manage devices connected to the computer, such as printers, scanners, mice and keyboards. Devices is not related to extending the display to a second monitor but to configuring device settings and preferences. Personalization is an option in the Windows settings that allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver.

QUESTION 264

A SOHO client is having trouble navigating to a corporate website. Which of the following should a technician do to allow access?
* Adjust the content filtering.
* Unmap port forwarding.
* Disable unused ports.
* Reduce the encryption strength

Content filtering is a process that manages or screens access to specific emails or webpages based on theircontent categories1. Content filtering can be used by organizations to control content access through their firewalls and enforce corporate policies around information system management2. A SOHO client may have content filtering enabled on their network and may need to adjust it to allow access to a corporate website that is blocked by default. The client can use a software program, a hardware device, or a subscription service to configure the content filtering settings andwhitelist the desired website2.

References: 1: Web content

filtering(https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=

2: What is Content Filtering? Definition and Types of Content Filters

(https://www.fortinet.com/resources/cyberglossary/content-filtering)

QUESTION 265

A user clicks a link in an email. A warning message in the user’s browser states the site’s certificate cannot be verified. Which of the following is the most appropriate action for a technician to take?
* Click proceed.
* Report the employee to the human resources department for violating company policy.
* Restore the computer from the last known backup.
* Close the browser window and report the email to IT security.

A warning message in the user’s browser stating the site’s certificate cannot be verified indicates that the site may be insecure, fraudulent, or malicious. This could be a sign of a phishing attempt, where the sender of the email tries to trick the user into clicking a link that leads to a fake website that mimics a legitimate one, in order to steal the user’s personal or financial information. The most appropriate action for a technician to take in this situation is to close the browser window and report the email to IT security, who can investigate the source and content of the email, and take the necessary steps to protect the user and the

network from potential harm. Clicking proceed could expose the user to malware, identity theft, or data breach. Reporting the employee to the human resources department for violating company policy is unnecessary and harsh, as the user may not have been aware of the phishing attempt or the company policy. Restoring the computer from the last known backup is premature and ineffective, as the user may not have been infected by anything, and the backup may not remove the email or the link from the user’s inbox

QUESTION 266

A technician is concerned about a large increase in the number of whaling attacks happening in the industry.

The technician wants to limit the company’s risk to avoid any issues. Which of the following items should the technician implement?
* Screened subnet
* Firewall
* Anti-phishing training
* Antivirus

Explanation

Anti-phishing training is a method of educating users on how to identify and avoid phishing attacks, which are attempts to trick users into revealing sensitive information or performing malicious actions by impersonating legitimate entities or persons. Whaling attacks are a specific type of phishing attack that target high-level executives or influential individuals within an organization. Anti-phishing training can help users recognize the signs of whaling attacks and prevent them from falling victim to them. Screened subnet, firewall, and antivirus are not items that can directly address the issue of whaling attacks.

QUESTION 267

A police officer often leaves a workstation for several minutes at a time. Which of the following is the BEST way the officer can secure the workstation quickly when walking away?
* Use a key combination to lock the computer when leaving.
* Ensure no unauthorized personnel are in the area.
* Configure a screensaver to lock the computer automatically after approximately 30 minutes of inactivity.
* Turn off the monitor to prevent unauthorized visibility of information.

Explanation

The BEST way to secure the workstation quickly when walking away is to use a key combination to lock the computer when leaving1