[2017 PDF&VCE Quickly Pass N10-006 Test With Lead2pass New N10-006 Brain Dumps (176-200)

Lead2pass 2017 September New CompTIA N10-006 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! CompTIA N10-006 exam is very popular in CompTIA field, many CompTIA candidates choose this exam to add their credentials. There are many resource online to offering CompTIA N10-006 exam questions, through many good feedbacks, we conclude that Lead2pass can help you pass your test easily with CompTIA N10-006 exam questions. Choose Lead2pass to get your CompTIA N10-006 certification. Following questions and answers are all new published by **CompTIA** Official Exam Center: https://www.lead2pass.com/n10-006.html QUESTION 176A company is looking for the simplest solution to help prioritize VoIP traffic on its congested network. Which of the following would BEST accomplish this? A. MPLSB. Caching enginesC. QoSD. Load balancingAnswer: CExplanation: QoS is the service where you can prioritize traffic running over one protocol as compared to the other. It is very similar to the term where you are opening a VIP queue for allowing that traffic to pass. QUESTION 177 Honeypots and honeynets are different in which of the following ways? A. Honeynets are managed collections of honeypots.B. Honeypots only test software security, not hardware.C. Honeynets require specialized hardware to implement.D. Honeypots are usually servers and honeynets are routers and switches. Answer: AExplanation:A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. QUESTION 178A corporate office recently had a security audit and the IT manager has decided to implement very strict security standards. The following requirements are now in place for each employee logging into the network: Biometric fingerprint scanComplex 12 character password5 digit pin code authorizationRandomized security question prompt upon login Which of the following security setups does this company employ? A. Single factor authenticationB. Three factor authenticationC. Two factor authenticationD. Single sign-on Answer: C Explanation: According to proponents, two-factor authentication could drastically reduce the incidence of online identity theft, phishing expeditions, and other online fraud, because the victim's password would no longer be enough to give a thief access to their information. QUESTION 179Which of the following wireless standards would BEST allow a company to utilize new and old devices on the 5GHz spectrum while allowing for the highest possible speeds? A. AB. BC. GD. N Answer: DExplanation: 802.11n is an amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output antennas (MIMO). 802.11n operates on both the 2.4 GHz and the lesser used 5 GHz bands QUESTION 180A technician has received a trouble ticket from a user who has intermittent wireless access. Moving the computer farther from the WAP results in a more stable connection. Which of the following is MOST likely the cause of this instability? A. Wrong encryption typeB. SSID mismatchC. Signal bounceD. Incorrect channel Answer: CExplanation:Bouncing is the tendency of any two metal contacts in an electronic device to generate multiple signals as the contacts close or open. QUESTION 181Which of the following is the MAXIMUM potential speed of CAT5e UTP cable? A. 10BaseTB. 100BaseTC. 100BaseFXD. 1000BaseT Answer: DExplanation: Category 5 e cable (Cat 5) is a twisted pair cable for carrying signals. This type of cable is used in structured cabling for computer networks such as Ethernet. The cable standard provides performance of up to 100 MHz and is suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), and 1000BASE-T (Gigabit Ethernet). QUESTION 182A technician sees suspicious traffic coming from a computer connected to a WAP. Which of the following can be used to stop this traffic while troubleshooting the problem? A. tracertB. QoSC. ipconfigD. MAC filtering Answer: DExplanation:By doing MAC filtering technician can block the data coming from a specific mac address. QUESTION 183Which of the following will BEST block a host from accessing the LAN on a network using static IP addresses? A. IP filteringB. Port filteringC. MAC address filteringD. DHCP lease Answer: A Explanation:IPFilter(commonly referred to asipf) is an open source software package that provides firewallservices and network address translation (NAT) for many UNIX-like operating systems. The author and software maintainer is Darren Reed. IPFilter supports both IPv4 and IPv6 protocols, and is a stateful firewall. QUESTION 184Which of the following remote access types requires a certificate for connectivity? A. SSHB. PPPC. HTTPSD. WEP Answer: AExplanation:Secure Shell(SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers that connects, via a secure channel over an insecure network, a server and a client (running SSH server and SSH client programs, respectively) QUESTION 185A network administrator is deploying a new wireless network with over 50 thin WAPs and needs to ensure all WAPs use consistent firmware and settings. Which of the following methods provides this functionality? A. Use WAP auto-configurationB. Use a wireless controllerC. Use PXE to load and track WAPsD. Use DHCP scope options Answer: BExplanation:A wireless controller is used in combination with the

Lightweight Access Point Protocol (LWAPP) to manage light-weight access points in large quantities by the network administrator ornetwork operations center. The wireless LAN controller is part of the Data Plane within the Cisco Wireless Model. The WLAN controller automatically handles the configuration of anywhere from 6 to 6000 wireless access-points, depending on the model. QUESTION 186The APIPA address 169.254.10.123 falls into which of the following class of addresses? A. AB. BC. CD. D Answer: BExplanation:As the range for class B is from 128.0.0.0 to 191.255.255.255 QUESTION 187An organization finds that most of the outgoing traffic on the network is directed at several Internet sites viewed by multiple computers simultaneously. Which of the following performance optimization methods would BEST alleviate network traffic? A. Load balancing internal web servers B. Redundant network resourcesC. Implement fault tolerance on the WAND. Implement caching engines Answer: D Explanation:A cache server is a dedicated network server or service acting as a server that saves Web pages or other Internet content locally. By placing previously requested information in temporary storage, or cache, a cache server both speeds up access to data and reduces demand on an enterprise's bandwidth. QUESTION 188A technician is troubleshooting Internet connectivity for a PC. Which of the following is MOST likely the reason for Internet connectivity issues upon inspecting the routing table? A. The router should be listed as 224.0.0.1B. The NIC is set to the wrong subnet maskC. The route of last resort is missingD. Loopback traffic is weighted higher than NIC interface traffic Answer: CExplanation:The default route is missing from the table.It looks like this:Network Destination Netmask Gateway Interface Metric0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.12 25 QUESTION 189 Compare the settings below to determine which of the following issues is preventing the user from connecting to a wireless network. Which of the following settings is incorrect on the client? A. The mode is incorrectB. SSID MismatchC. Incorrect WEP Key D. Channel is set incorrectly Answer: BExplanation:the first thing which will be checked is the SSID and it is case sensitive but in the above shown example, it is not same so it will stop user from connecting. QUESTION 190A technician replaces a failed router in an office with the same model unit using the default settings. After the installation, the technician reboots all of the PCs and servers. Upon reboot some of the PCs are receiving IP addresses on the same subnet as the new router; other PCs are receiving addresses on the same subnet as the servers. Which of the following most likely describes the issue? A. The DHCP lease pool was not large enoughB. DHCP lease times were set too lowC. The router is not the only DHCP serverD. DHCP was not enabled on the replacement router Answer: CExplanation:This happens when there are multiple DHCP servers in the same LAN subnet. Here some machines are getting ip address from the router while some are getting ip address from another DHCP server present in the same domain. QUESTION 191A technician is troubleshooting authentication issues on a server. It turns out the clock on the server was 72 minutes behind. Setting the clock to the correct time fixed the issue. Given the scenario, which of the following authentication methods was being used? A. KerberosB. CHAPC. TACACS+D. RADIUS Answer: AExplanation:Kerberos is a distributed authentication service that allows a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server, or just server) without sending data across the network that might allow an attacker or theverifier to subsequently impersonate the principal. Kerberos optionally provides integrity and confidentiality for data sent between the client and server. QUESTION 192Which of the following wireless standards uses a block encryption cipher rather than a streamcipher? A. WPA2-CCMPB. WPAC. WEPD. WPA2-TKIP Answer: AExplanation:Counter Cipher Mode with Block Chaining Message Authentication Code Protocol or CCMP (CCM mode Protocol) is an encryption protocol designed for Wireless LAN products that implement the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES standard. It was created to address the vulnerabilities presented by WEP, a dated, insecure protocol. QUESTION 193Which of the following is the OSI layer that handles file compression such as LZMA or DEFLATE? A. Layer 3B. Layer 5C. Layer 6D. Layer 7 Answer: CExplanation:The presentation level is translator between the application and network format. Unlike the lower layers, its concern is with the syntax and semantics of the informationtransmitted. Most user programs do not exchange random binary bit strings. They exchange data such as names, addresses, dates, etc. Different computers store the data in a different way. In order to allow these computers to transmit the data to each other the presentation layer translates the data into a standard form to be used on the network. Another function is data compression which can be used to reduce the number of bits needed to send the packet of information. Security is also added at this layer by using data encryption and decryption. This prevents others from intercepting the data and being able to decipher the meaning of the bits. QUESTION 194A network administrator is performing a penetration test on the WPA2 wireless network. Which of the following can be used to find the key? A. DoSB. Buffer overflowC. Dictionary fileD. SQL injection Answer: CExplanation:A file used by the debugger. It contains information about a program's structure and contents. The Compiler creates the dictionary file in the first phase of compilation, when checking the syntax. A dictionary file has the filename extension.idy, and is often referred to an.idyfile. QUESTION 195Which of the following can be used to compromise a WPA encrypted wireless network when therainbow table does not contain the key? A. Evil

twinB. War chalkingC. Buffer overflowD. Virus Answer: AExplanation:An evil twin is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider.This type of evil twin attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there. QUESTION 196A system administrator is implementing an IDS on the database server to see who is trying to access the server. The administrator relies on the software provider for what to detect. Which of the following would MOST likely be installed? A. Behavior based IDS B. Network based IDSC. Signature based IDSD. Honeypot Answer: CExplanation:Signature detection involves searching network traffic for a series of bytes or packet sequences known to be malicious. A key advantage of this detection method is that signatures are easy to develop and understand if you know what network behavior you're trying to identify. QUESTION 197A vendor releases an emergency patch that fixes an exploit on their network devices. The network administrator needs to quickly identify the scope of the impact to the network. Which of the following should have been implemented? A. Change managementB. Asset managementC. Network snifferD. System logs Answer: BExplanation:Assetmanagement is defined as the business practice of managing and optimizing the purchase, deployment, maintenance, utilization, and disposal of hardware and software applications within an organization. QUESTION 198Which of the following can be described as a DoS attack? A. Disabling a specific system and making it unavailable to usersB. Implementing a keyloggerC. Intercepting a packet and decrypting the contentsD. Communicating with employees to get company information Answer: AExplanation:A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet. QUESTION 199A user is connecting to the Internet at an airport through an ad-hoc connection. Which of the following is the MOST likely security threat? A. Man-in-the-middleB. Social engineeringC. Phishing D. DoS Answer: AExplanation:A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. QUESTION 200An application server is placed on the network and the intended application is not working correctly. Which of the following could be used to make sure sessions are being opened properly? A. Antivirus scannerB. IDSC. Packet snifferD. Toner probe Answer: CExplanation:Packet Sniffer is a tool that can help you locate network problems by allowing you to capture and view the packet level data on your network.So we can capture the session and find the cause of failure. More free Lead2pass **N10-006** exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDVzI0bUdJdU1ESkk CompTIA N10-006 exam questions are available in PDF and VCE format. This makes it very convenient for you to follow the course and study the exam whenever and wherever you want. The CompTIA N10-006 exam questions follow the exact paper pattern and question type of the actual N10-006 certification exam, it lets you recreate the exact exam scenario, so you are armed with the correct information for the N10-006 certification exam. 2017 **CompTIA N10-006** (All 1521 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/n10-006.html [100% Exam Pass Guaranteed]