[2017 PDF&VCE Lead2pass N10-006 Dumps PDF Free Download (201-225)

Lead2pass 2017 September New CompTIA N10-006 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Lead2pass presents the highest quality of N10-006 exam question which helps candidates to pass the N10-006 exams in the first attempt. Lead2pass professional tools like questions and answers are extremely reliable source of preparation. When you use Lead2pass preparation products your success in the Certification exam is guaranteed. Following questions and answers are all new published by **CompTIA** Official Exam Center: https://www.lead2pass.com/n10-006.html QUESTION 201Which of the following provides secure access to a network device? A. SNMPv2B. FTPC. RSHD. SSHAnswer: DExplanation: 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 202Which of the following uses distance vector algorithms to determine the BEST network route to a destination address? A. IS-ISB. OSPFC. BGPD. RIP Answer: DExplanation: Here the termdistance vectorrefers to the fact that the protocol manipulatesvectors (arrays) of distances to other nodes in the network QUESTION 203Which of the following uses classless subnet masks across a network? A. SubnettingB. CIDRC. SupernettingD. Summarization Answer: BExplanation:Classless Inter-Domain Routing is based onvariable-length subnet masking(VLSM), which allows a network to be divided into variously sized subnets, providing the opportunity to size a network more appropriately for local needs and also CIDR allows an address or routing prefix to be written with a suffix indicating the number of bits of the prefix, such as 192.168.2.0/24. QUESTION 204Enterprise IP routing policy is MOST clearly depicted in which of the following configuration management documents? A. Logical network diagramsB. Physical network diagramsC. Wiring schematicsD. Group security role assignments Answer: AExplanation:A logical network diagram illustrates the network architecture of a group of interconnected computers and other devices, such as printers, modems, switches, routers, and even mobile devices. These electronic components form the physical network that provides local area network (LAN) and wide area network (WAN) access to users. Once you know the layout and you have an idea about the packet flow then your job becomes easy and you can create an action plan to go for the implementation. QUESTION 205While preparing to replace an old CAT3 cable with a CAT6 cable to implement VoIP, a facilities employee mistakenly disconnects the entire patch panel, including valid wiring to live workstations. Which of the following should an administrator use in order to connect those ports FIRST? A. TonerB. MultimeterC. ReflectometerD. Cable tester Answer: AExplanation: Toner-connects to any voice, data, or video cable to detect open/short circuits, continuity, AC/DC voltage* and dial tone* all while protecting up to 52 volt. QUESTION 206Which of the following methods would be implemented to correct a network slowdown caused by excessive video streaming? A. Traffic shapingB. Proxy serverC. VPN concentratorD. High availability Answer: AExplanation:As traffic shaping will prioritize the video packets over another packets and then video packets will travel fast on bandwidth. QUESTION 207While working on a PC, a technician notices 0.0.0.0 in the routing table. Which of the following does this indicate? A. It is the default route.B. This is the address for the DHCP server.C. The PC has not been assigned an IP address.D. The firewall is down. Answer: AExplanation: The address 0.0.0.0 generally means "any address". If a packet destination doesn't match an individual address in the table, it must match a 0.0.0.0 gateway address. In other words, default gateway is always pointed by 0.0.0.0 QUESTION 208Users inform an administrator that the network is slow. The administrator notices the bulk of the traffic is SIP and RTP traffic. Which of the following could the administrator do to help BEST alleviate the traffic congestion for the users? A. Create an ACL on the switches and routers that are dropping SIP and RTP packets.B. Create a QoS policy prioritizing users over RTP and SIP traffic.C. Create another VLAN for SIP and RTP traffic.D. Create a rule to throttle SIP and RTP to 10Kbps or less. Answer: CExplanation:As if we will create a vlan for sip and rtp traffic only this traffic will flow from the ports then. QUESTION 209If a NIC does not have a link light, there is a failure at which of the following OSI layers? A. PhysicalB. SessionC. Data linkD. Presentation Answer: AExplanation: The NIC does not have light refers to a situation that there could be a fault in the LAN cable or the ports are down and all of these fall under the physical layer. To make it simple, it falls in physical layer because blinking lights refers to the physical connectivity. QUESTION 210Which of the following is the control when observing network bandwidth patterns over time? A. Network logB. BaselineC. Flow dataD. Interface statistics Answer: BExplanation:To successfully baseline a network it is important to consider two functions; performance at protocol level and performance at application level. There are many significant metrics to consider at the protocol level, but only a few which are critical. The most important is bandwidthutilizationcompared with bandwidth availability. The most likely cause of poor network performance is insufficient bandwidth. Trending bandwidthutilizationallows you torecognizeproblem areas, provide enough bandwidth to reach performance objectives, and predict future capacity requirements. Changes in bandwidthutilizationpatterns also provide a clear indication of network usage alterations,

such as a change in end-userbehavior, or theunauthorizedaddition of an application. QUESTION 211Which of the following technologies is used on cellular networks? A. EthernetB. CDMAC. CSMA/CAD. POTS Answer: BExplanation:CDMA is an example of multiple access, which is where several transmitters can send information simultaneously over a single communication channel. This allows several users to share a band of frequencies (see bandwidth). To permit this to be achieved without undue interference between the users CDMA employs spread-spectrum technology and a special coding scheme QUESTION 212Which of the following technologies allows multiple staff members to connect back to a centralized office? A. Peer to PeerB. VPNC. PKID. VLAN Answer: BExplanation: VPNenables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-pointconnection through the use of dedicated connections, encryption, or a combination of the two. QUESTION 213Which of the following is the MOST secure way to prevent malicious changes to a firewall? A. SNMPv2 access onlyB. TELNET access onlyC. SSH access onlyD. Console access only Answer: D QUESTION 214Which of the following allows a malicious attacker to view network traffic if the attacker is on the same network segment as Joe, an administrator? A. DoS attackB. Man-in-the-middle attackC. Smurf attackD. Xmas attack Answer: BExplanation:An attack where a user gets between the sender and receiver of information and sniffs any information being sent. In some cases, users may be sending unencrypted data, which means theman-in-the-middle(MITM) can obtain any unencrypted information. In other cases, a user may be able to obtain information from the attack, but have to unencrypt the information before it can be read. QUESTION 215Which of the following OSI layers allows users to access network services such as file sharing? A. Layer 1B. Layer 3C. Layer 4D. Layer 7 Answer: DExplanation:Basically File Transfer protocol(FTP) is responsible for file transfer which lies under Application layer (Layer 7) of OSI layers. QUESTION 216Which of the following can function in an unsecure mode? A. SNMPv3B. SSHC. SSLD. SCP Answer: AExplanation: SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, it looks much different due to new textual conventions, concepts, and terminology.SNMPv3 primarily added security and remote configuration enhancements to SNMP QUESTION 217Which of the following is used to register and resolve IP addresses with their plain language equivalents? A. Proxy serverB. DNS serverC. Brouter equipmentD. DHCP server Answer: BExplanation: DNS server translate (resolution) the human-memorable domain names and hostnames into the corresponding numeric Internet Protocol (IP) addresses. QUESTION 218An administrator determines there are an excessive number of packets being sent to a web server repeatedly by a small number of external IP addresses. This is an example of which of the following attacks? A. DDoSB. VirusesC. WormsD. Man-in-the-middle Answer: AExplanation:DDoS attack,a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as thePing of DeathandTeardropattacks, exploit limitations in the TCP/IP protocols QUESTION 219Which of the following features will a firewall MOST likely use to detect and prevent malicious traffic on the network? A. Zone filteringB. Signature identificationC. Port identificationD. Port scanner Answer: BExplanation:Signature-based detection really is more along the lines of intrusion detection than firewalls. However, many personal firewalls and some corporate firewalls contain this functionality. Essentially, the system can be configured to look for specific patterns, known to be malicious, and block the traffic QUESTION 220Which of the following protocols is MOST commonly associated with VoIP? A. LDAPB. HTTPSC. SIPD. SCP Answer: CExplanation:The Session Initiation Protocol (SIP) is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks. QUESTION 221Stateful packet inspection is a security technology used by which of the following devices? A. Unmanaged switchB. Hardware firewallC. BridgeD. IDS Answer: BExplanation:With Stateful Packet Inspection (SPI), every time a packet is sent out of the computer, the firewall keeps track of it. When a packet comes back to the firewall, the firewall can tell whether or not the in-bound packet is a reply to the packet that was sent out.This way, the firewall can handle most network traffic safely without a complex configuration of firewall rules. QUESTION 222Which of the following commands will provide an administrator with the number of hops a packet takes from host to host? A. nslookupB. pingC. tracerouteD. route Answer: CExplanation:In computing, traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop indicates the total time spent to establish the connection. QUESTION 223Which of the following is needed when using WPA2-Enterprise wireless encryption? A. TFTPB. RADIUSC. LDAPD. IPSec Answer: BExplanation:The WPA2 standard supports two different authentication mechanisms: one using standard RADIUS servers and the other with a shared key, similar to how WEP works. QUESTION 224Which of the following technologies is used to connect public networks using POTS lines? A. OC3B. OC12C. PSTND. Cable Answer: CExplanation: The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, cellular

networks, communications satellites, and undersea telephone cables, all interconnected by switching centers, thus allowing any telephone in the world to communicate with any other QUESTION 225An administrator would like to inspect all traffic flowing over the SMTP protocol on a given network. Which of the following tools would accomplish this? (Select TWO). A. Packet snifferB. HoneypotC. Port mirroringD. IPSE. Port scannerF. IDS Answer: ACExplanation:(IPS), also known asintrusion detection and prevention systems(IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.And we use packet sniffer to detect the types of packet. More free Lead2pass **N10-006** exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDVzI0bUdJdU1ESkk Lead2pass is now here to help you with your N10-006 exam certification problems. Because we are the best N10-006 exam questions training material providing vendor, all of our candidates get through N10-006 exam without any problem. **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]