[Lead2pass Official 210-260 Exam Dumps Free Download In Lead2pass 100% 210-260 Exam Questions (201-220)

2017 September Cisco Official New Released 210-260 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Amazing,100% candidates have passed the 210-260 exam by practising the preparation material of Lead2pass, because the braindumps are the latest and cover every aspect of 210-260 exam. Download the braindumps for an undeniable success in 210-260 exam. Following questions and answers are all new published by Cisco Official Exam Center: https://www.lead2pass.com/210-260.html QUESTION 201What is example of social engineering A. Gaining access to a building through an unlocked door.B. something about inserting a random flash drive.C. gaining access to server room by posing as ITD. watching you enter your user and password on a network computer (something to that effect) Answer: C QUESTION 202Which port should (or would) be open if VPN NAT-T was enabled? A. port 4500 outside interfaceB. port 4500 in all interfaces where ipsec usesC. port 500D. port 500 outside interface Answer: BExplanation:NAT traversal: The encapsulation of IKE and ESP in UDP port 4500 enables these protocols to pass through a device or firewall performing NAT. https://en.wikipedia.org/wiki/Internet_Key_Exchangehttps://supportforums.cisco.com/document/64281/how-does-nat-t-work-ipsec QUESTION 203Diffie-Hellman key exchange question A. IKEB. IPSECC. SPAND. STP Answer: AExplanation: https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange QUESTION 204Security well known terms Choose 2 A. TrojanB. PhishingC. Something LCD. Ransomware Answer: BDExplanation:The following are the most common types of malicious software:+ Computer viruses+ Worms+ Mailers and mass-mailer worms+ Logic bombs+ Trojan horses+ Back doors+ Exploits+ Downloaders+ Spammers+ Key loggers+ Rootkits+ Ransomware QUESTION 205What's the technology that you can use to prevent non malicious program to run in the computer that is disconnected from the network? A. FirewallB. Software AntivirusC. Network IPSD. Host IPS. Answer: D QUESTION 206What command could you implement in the firewall to conceal internal IP address? A. no source-routeB. no broadcast.. ..C. no proxy-arpD. no cdp run Answer: CExplanation:The Cisco IOS software uses proxy ARP (as defined in RFC 1027) to help hosts with no knowledge of routing determine the media addresses of hosts on other networks or subnets. For example, if the router receives an ARP request for a host that is not on the same interface as the ARP request sender, and if the router has all of its routes to that host through other interfaces, then it generates a proxy ARP reply packet giving its own local data-link address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host. Proxy ARP is enabled by default.Router(config-if)# ip proxy-arp - Enables proxy ARP on the interface.http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfipadr.html#wp1001233 QUESTION 207Which statement about college campus is true? A. College campus has geographical position.B. College campus Hasn`t got internet access.C. College campus Has multiple subdomains. Answer: A QUESTION 208Which firepower preprocessor block traffic based on IP? A. Signature-BasedB. Policy-BasedC. Anomaly-BasedD. Reputation-Based Answer: DExplanation:Access control rules within access control policies exert granular control over network traffic logging and handling. Reputation-based conditions in access control rules allow you to manage which traffic can traverse your network, by contextualizing your network traffic and limiting it where appropriate. Access control rules govern the following types of reputation-based control:+ Application conditions allow you to perform application control, which controls application traffic based on not only individual applications, but also applications' basic characteristics: type, risk, business relevance, categories, and tags.+ URL conditions allow you to perform URL filtering, which controls web traffic based on individual websites, as well as websites' system-assigned category and reputation.The ASA FirePOWER module can perform other types of reputation-based control, but you do not configure these using access control rules. For more information, see:+ Blacklisting Using Security Intelligence IP Address Reputation explains how to limit traffic based on the reputation of a connection's origin or destination as a first line of defense.+ Tuning Intrusion Prevention Performance explains how to detect, track, store, analyze, and block the transmission of malware and other types of prohibited files. http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/AC-Rules-App-URL-Reputation.html QUESTION 209Which two NAT types allow only objects or groups to reference an IP address? (Choose two) A. dynamic NATB. dynamic PATC. static NATD. identity NAT Answer: ACExplanation:Adding Network Objects for Mapped AddressesFor dynamic NAT, you must use an object or group for the mapped addresses. Other NAT types have the option of using inline addresses, or you can create an object or group according to this section.* Dynamic NAT:+ You cannot use an inline address; you must configure a network object or group.+ The object or group cannot contain a subnet; the object must define a range; the group can include hosts and ranges.+ If a mapped network object contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback.* Dynamic PAT

(Hide):+ Instead of using an object, you can optionally configure an inline host address or specify the interface address.+ If you use an object, the object or group cannot contain a subnet; the object must define a host, or for a PAT pool, a range; the group (for a PAT pool) can include hosts and ranges.* Static NAT or Static NAT with port translation:+ Instead of using an object, you can configure an inline address or specify the interface address (for static NAT-with-port-translation).+ If you use an object, the object or group can contain a host, range, or subnet.* Identity NAT+ Instead of using an object, you can configure an inline address.+ If you use an object, the object must match the real addresses you want to translate.
http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ nat_objects.html#61711 QUESTION 210What port option in a PVLAN that can communicate with every other ports... A. Promiscuous..B. Community portsC. Ethernet portsD. Isolate ports Answer: AExplanation:+ Promiscuous -- A promiscuous port belongs to the primary VLAN. The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN.+ Isolated -- An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports+ Community -- A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html QUESTION 211Which command enable ospf authentication? A. ip ospf authentication message-digestB. network 192.168.10.0 0.0.0.255 area 0C. area 20 authentication message-digestD. ip ospf message-digest-key 1 md5 CCNA Answer: A Explanation:This question might be incomplete. Both ip ospf authentication message-digest and area 20 authentication message-digest command enable OSPF authentication through MD5.Use the ip ospf authentication-key interface command to specify this password. If you enable MD5 authentication with the message-digest keyword, you must configure a password with the ip ospf message- digest-key interface command.interface GigabitEthernet0/1ip address 192.168.10.1 255.255.255.0ip ospf authentication message-digestip ospf message-digest-key 1 md5 CCNACisco Official Certification Guide, Implement Routing Update Authentication on OSPF, p.348 To enable authentication for an OSPF area, use the area authentication command in router configuration mode.To remove an authentication specification of an area or a specified area from the configuration, use the no form of this command.area area-id authentication [message-digest]no area area-id authentication [message-digest]
http://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfospf.html
https://supportforums.cisco.com/document/22961/ospf-authentication QUESTION 212Which NAT option is executed first during in case of multiple nat translations? A. dynamic nat with shortest prefixB. dynamic nat with longest prefixC. static nat with shortest prefixD. static nat with longest prefix Answer: D QUESTION 213Which security term refers to a person, property, or data of value to a company? A. RiskB. AssetC. Threat preventionD. Mitigation technique Answer: B QUESTION 214 Which option is a weakness in an information system that an attacker might leverage to gain unauthorized access to the system or its data? A. hackB. mitigationC. riskD. vulnerabilityE. exploit Answer: DExplanation:A flaw or weakness in a system's design or implementation that could be exploited. QUESTION 215What show command can see vpn tunnel establish with traffic passing through? A. show crypto ipsec saB. show crypto sessionC. show crypto isakmp saD. show crypto ipsec transform-set Answer: AExplanation:#show crypto ipsec sa - This command shows IPsec SAs built between peers In the output you see#pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0#pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0which means packets are encrypted and decrypted by the IPsec peer.
http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#ipsec_sa
QUESTION 216which will auto-nat process first (the focus is on auto-nat)? A. dynamic Nat shortest prefixB. dynamic nat longest prefixC. static nat shortest prefixD. static nat longest prefix Answer: D QUESTION 217Where OAKLEY and SKEME come to play? A. IKEB. ISAKMPC. DES Answer: AExplanation:The Oakley Key Determination Protocol is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie¬Hellman key exchange algorithm.The protocol was proposed by Hilarie K. Orman in 1998, and formed the basis for the more widely used Internet key exchange protocolhttps://en.wikipedia.org/wiki/Oakley_protocolIKE (Internet Key Exchange)A key management protocol standard that is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside of the Internet Security Association and Key Management Protocol (ISAKMP) framework.ISAKMP, Oakley, and Skeme are security protocols implemented by IKE

https://www.symantec.com/security_response/glossary/define.jsp?letter=i&word=ike-internet-key- exchange QUESTION 218What does the key length represent A. Hash block sizeB. Cipher block sizeC. Number of permutations Answer: CExplanation:In cryptography, an algorithm's key space refers to the set of all possible permutations of a keys.If a key were eight bits (one byte) long, the keyspace would consist of 28 or 256 possible keys. Advanced Encryption Standard (AES) can use a symmetric key of 256 bits, resulting in a key space containing 2256 (or 1.1579 × 1077) possible keys.https://en.wikipedia.org/wiki/Key_space_(cryptography) QUESTION 219Which type of attack is directed against the network directly? A. Denial of ServiceB. phishingC. trojan horse Answer: AExplanation:Denial of service refers to willful attempts to disrupt legitimate users from getting access to the resources they intend to. Although no complete solution exists, administrators can do specific things to protect the network from a DoS attack and to lessen its effects and prevent a would-be attacker from using a system as a source of an attack directed at other systems. These mitigation techniques include filtering based on bogus source IP addresses trying to come into the networks and vice versa. Unicast reverse path verification is one way to assist with this, as are access lists. Unicast reverse path verification looks at the source IP address as it comes into an interface, and then looks at the routing table. If the source address seen would not be reachable out of the same interface it is coming in on, the packet is considered bad, potentially spoofed, and is dropped. QUESTION 220With which technology do apply integrity, confidentially and authenticate the source A. IPSecB. IKEC. Certificate authorityD. Data encryption standards Answer: AExplanation:IPsec is a collection of protocols and algorithms used to protect IP packets at Layer 3 (hence the name of IP Security [IPsec]). IPsec provides the core benefits of confidentiality through encryption, data integrity through hashing and HMAC, and authentication using digital signatures or using a pre-shared key (PSK) that is just for the authentication, similar to a password. You can pass Cisco 210-260 exam if you get a complete hold of 210-260 braindumps in Lead2pass. What's more, all the 210-260 Certification exam Q and As provided by Lead2pass are the latest. 210-260 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDYUk3WWFWOEhsSU0 2017 Cisco 210-260 exam dumps (All 362 Q&As) from Lead2pass: https://www.lead2pass.com/210-260.html [100% Exam Pass Guaranteed]