[February 2018 Lead2pass 100% Valid 210-260 Exam Questions PDF Free Download 368q

Lead2pass 2018 100% Real 210-260 Exam Questions: https://www.lead2pass.com/210-260.html QUESTION 11What features can protect the data plane? (Choose three.) A. policingB. ACLsC. IPSD. antispoofingE. QoSF. DHCP-snoopingAnswer: BDF Explanation:Data Plane SecurityData plane security can be implemented using the following features:Access control listsAccess control lists (ACLs) perform packet filtering to control which packets move through the network and where.AntispoofingACLs can be used as an antispoofing mechanism that discards traffic that has an invalid source address.Layer 2 security featuresCisco Catalyst switches have integrated features to help secure the Layer 2 infrastructure.ACLsACLs are used to secure the data plane in a variety of ways, including the following:Block unwanted traffic or usersACLs can filter incoming or outgoing packets on an interface, controlling access based on source addresses, destination addresses, or user authentication.Reduce the chance of DoS attacksACLs can be used to specify whether traffic from hosts, networks, or users can access the network. The TCP intercept feature can also be configured to prevent servers from being flooded with requests for a connection.Mitigate spoofing attacksACLs enable security practitioners to implement recommended practices to mitigate spoofing attacks.Provide bandwidth controlACLs on a slow link can prevent excess traffic.Classify traffic to protect other planesACLs can be applied on vty lines (management plane).ACLs can control routing updates being sent, received, or redistributed (control plane).AntispoofingImplementing the IETF best current practice 38 (BCP38) and RFC 2827 ingress traffic filtering renders the use of invalid source IP addresses ineffective, forcing attacks to be initiated from valid, reachable IP addresses which could be traced to the originator of an attack.Features such as Unicast Reverse Path Forwarding (uRPF) can be used to complement the antispoofing strategy.Layer 2 Data Plane ProtectionThe following are Layer 2 security tools integrated into the Cisco Catalyst switches:Port securityPrevents MAC address spoofing and MAC address flooding attacks DHCP snoopingPrevents client attacks on the Dynamic Host Configuration Protocol (DHCP) server and switch Dynamic ARP inspection (DAI)Adds security to ARP by using the DHCP snooping table to minimize the impact of ARP poisoning and spoofing attacksIP source guardPrevents IP spoofing addresses by using the DHCP snooping table QUESTION 12How many crypto map sets can you apply to a router interface? A. 3B. 2C. 4D. 1 Answer: D QUESTION 13What is the transition order of STP states on a Layer 2 switch interface? A. listening, learning, blocking, forwarding, disabledB. listening, blocking, learning, forwarding, disabledC. blocking, listening, learning, forwarding, disabledD. forwarding, listening, learning, blocking, disabled Answer: CExplanation:The ports on a switch with enabled Spanning Tree Protocol (STP) are in one of the following five port states. BlockingListeningLearningForwardingDisabledA switch does not enter any of these port states immediately except the blocking state. When the Spanning Tree Protocol (STP) is enabled, every switch in the network starts in the blocking state and later changes to the listening and learning states.Blocking StateThe Switch Ports will go into a blocking state at the time of election process, when a switch receives a BPDU on a port that indicates a better path to the Root Switch (Root Bridge), and if a port is not a Root Port or a Designated Port.A port in the blocking state does not participate in frame forwarding and also discards frames received from the attached network segment. During blocking state, the port is only listening to and processing BPDUs on its interfaces. After 20 seconds, the switch port changes from the blocking state to the listening state.Listening StateAfter blocking state, a Root Port or a Designated Port will move to a listening state. All other ports will remain in a blocked state. During the listening state the port discards frames received from the attached network segment and it also discards frames switched from another port for forwarding. At this state, the port receives BPDUs from the network segment and directs them to the switch system module for processing. After 15 seconds, the switch port moves from the listening state to the learning state.Learning StateA port changes to learning state after listening state. During the learning state, the port is listening for and processing BPDUs . In the listening state, the port begins to process user frames and start updating the MAC address table. But the user frames are not forwarded to the destination. After 15 seconds, the switch port moves from the learning state to the forwarding state.Forwarding StateA port in the forwarding state forwards frames across the attached network segment. In a forwarding state, the port will process BPDUs , update its MAC Address table with frames that it receives, and forward user traffic through the port. Forwarding State is the normal state. Data and configuration messages are passed through the port, when it is in forwarding state.Disabled StateA port in the disabled state does not participate in frame forwarding or the operation of STP because a port in the disabled state is considered non-operational. QUESTION 14Which sensor mode can deny attackers inline? A. IPSB. fail-closeC. IDSD. fail-open Answer: A QUESTION 15Which options are filtering options used to display SDEE message types? A. stopB. noneC. errorD. all Answer: CD QUESTION 16When a company puts a security policy in place, what is the effect on the company's business? A. Minimizing risk B. Minimizing total cost of ownershipC. Minimizing liabilityD. Maximizing compliance Answer: A QUESTION 17Which wildcard mask is associated with a subnet mask of /27? A. 0.0.0.31B. 0.0.0.27C. 0.0.0.224D. 0.0.0.255 Answer: A

QUESTION 18Which statements about reflexive access lists are true? A. Reflexive access lists create a permanent ACEB. Reflexive access lists approximate session filtering using the established keywordC. Reflexive access lists can be attached to standard named IP ACLsD. Reflexive access lists support UDP sessionsE. Reflexive access lists can be attached to extended named IP ACLsF. Reflexive access lists support TCP sessions Answer: DEF QUESTION 19Which actions can a promiscuous IPS take to mitigate an attack? A. modifying packetsB. requesting connection blockingC. denying packetsD. resetting the TCP connectionE. requesting host blockingF. denying frames Answer: BDEExplanation:Promiscuous Mode Event ActionsThe following event actions can be deployed in Promiscuous mode. These actions are in affect for a user- configurable default time of 30 minutes. Because the IPS sensor must send the request to another device or craft a packet, latency is associated with these actions and could allow some attacks to be successful.Blocking through usage of the Attack Response Controller (ARC) has the potential benefit of being able to perform to the network edge or at multiple places within the network.Request block host: This event action will send an ARC request to block the host for a specified time frame, preventing any further communication. This is a severe action that is most appropriate when there is minimal chance of a false alarm or spoofing.Request block connection: This action will send an ARC response to block the specific connection. This action is appropriate when there is potential for false alarms or spoofing. Reset TCP connection: This action is TCP specific, and in instances where the attack requires several TCP packets, this can be a successful action. However, in some cases where the attack only needs one packet it may not work as well. Additionally, TCP resets are not very effective with protocols such as SMTP that consistently try to establish new connections, nor are they effective if the reset cannot reach the destination host in time.Event actions can be specified on a per signature basis, or as an event action override (based on risk rating values ?event action override only). In the case of event action override, specific event actions are performed when specific risk rating value conditions are met. Event action overrides offer consistent and simplified management. IPS version 6.0 contains a default event action override with a deny-packet-inline action for events with a risk rating between 90 and 100. For this action to occur, the device must be deployed in Inline mode.Protection from unintended automated action responsesAutomated event actions can have unintended consequences when not carefully deployed. The most severe consequence can be a self denial of service (DoS) of a host or network. The majority of these unintended consequences can be avoided through the use of Event Action Filters, Never Block Addresses, Network spoofing protections, and device tuning. The following provides an overview of methods used to prevent unintended consequences from occurring.Using Event Action Filters and Never BlockBy using these capabilities, administrators may prevent a miscreant from spoofing critical IP addresses, causing a self inflicted DoS condition on these critical IP addresses. Note that Never Block capabilities only apply to ARC actions. Actions that are performed inline will still be performed as well as rate limiting if they are configured.Minimize spoofingAdministrators can minimize spoofed packets that enter the network through the use of Unicast Reverse Path Forwarding. Administrators can minimize spoofing within their network through the use of IP Source Guard. The white paper titled Understanding Unicast Reverse Path Forwarding provides details on configuration of this feature. More information on IP Source Guard is available in the document titled Configuring DHCP Features and IP Source Guard. Careful Use of Event ActionsBy judicious use of event actions that block unwanted traffic, such as using the high signature fidelity rating, and not using automated actions on signatures that are easily spoofed, administrators can reduce the probability of an unintended result. For an event to have a high risk rating, it must have a high signature fidelity rating unless the risk rating is artificially increased through the use of Target Value Rating or Watch List Rating, which are IP specific increases.TuningBy tuning the signature set to minimize false positive events, administrators can reduce the chance of an event action that has an unintended consequence.High Base Risk Rating EventsIn most cases, events with a high base risk rating or a high signature fidelity rating are strong candidates for automated event actions. Care should be taken with protocols that are easily spoofed in order to prevent self DoS conditions. QUESTION 20Which Cisco Security Manager application collects information about device status and uses it to generate notifications and alerts? A. FlexConfigB. Device ManagerC. Report ManagerD. Health and Performance Monitor Answer: DExplanation:"Report Manager - Collects, displays and exports network usage and security information for ASA and IPS devices, and for remote-access IPsec and SSL VPNs. These reports aggregate security data such as top sources, destinations, attackers, victims, as well as security information such as top bandwidth, duration, and throughput users. Data is also aggregated for hourly, daily, and monthly periods." and"Health and Performance Monitor (HPM) ?Monitors and displays key health, performance and VPN data for ASA and IPS devices in your network. This information includes critical and non-critical issues, such as memory usage, interface status, dropped packets, tunnel status, and so on. You also can categorize devices for normal or priority monitoring, and set different alert rules for the priority devices." **210-260 dumps full version (PDF&VCE):**
https://www.lead2pass.com/210-260.html Large amount of free **210-260** exam questions on Google Drive:
https://drive.google.com/open?id=0B3Syig5i8gpDYUk3WWFWOEhsSU0