PassLeader Offer The Highest Coverage Rate Of Real 350-018 Exam Questions (21-40)

QUESTION 21 An attacker configures an access point to broadcast the same SSID that is used at a public hot- spot, and launches a deauthentication attack against the clients that are connected to the hot-spot, with the hope that the clients will then associate to the AP of the attacker. In addition to the deauthentication attack, what attack has been launched? A.&#160;&#160;&#160; man-in-the-middle B.&#160;&#160;&#160; MAC spoofing C.&#160;&#160;&#160; Layer 1 DoS D.&#160;&#160;&#160; disassociation attackAnswer: A QUESTION 22 Which statement best describes the concepts of rootkits and privilege escalation? A.&#160;&#160;&#160; Rootkits propagate themselves. B.&#160;&#160;&#160; Privilege escalation is the result of a rootkit. C.&#160;&#160;&#160; Rootkits are a result of a privilege escalation. D.&#160;&#160;&#160; Both of these require a TCP port to gain access. Answer: B QUESTION 23 Which multicast capability is not supported by the Cisco ASA appliance? A.&#160;&#160;&#160; ASA configured as a rendezvous point B.&#160;&#160;&#160; sending multicast traffic across a VPN tunnel C.&#160;&#160;&#160; NAT of multicast traffic D.&#160;&#160;&#160; IGMP forwarding (stub) mode Answer: B QUESTION 24 Which method of output queuing is supported on the Cisco ASA appliance? A.&#160;&#160;&#160; CBWFQ B.&#160;&#160;&#160; priority queuing C.&#160;&#160;&#160; MDRR D.&#160;&#160;&#160; WFQ E.&#160;&#160;&#160; custom queuing Answer: B QUESTION 25 Which four values can be used by the Cisco IPS appliance in the risk rating calculation? (Choose four.) A.&#160;&#160;&#160; attack severity rating B.&#160;&#160;&#160; target value rating C.&#160;&#160;&#160; signature fidelity rating D.&#160;&#160;&#160; promiscuous delta E.&#160;&#160;&#160; threat rating F.&#160;&#160;&#160; alert rating Answer: ABCD QUESTION 26 Which three authentication methods does the Cisco IBNS Flexible Authentication feature support? (Choose three.) A.&#160;&#160;&#160; cut-through proxy B.&#160;&#160;&#160; dot1x C.&#160;&#160;&#160; MAB D.&#160;&#160;&#160; SSO E.&#160;&#160;&#160; web authentication Answer: BCE QUESTION 27 Troubleshooting the web authentication fallback feature on a Cisco Catalyst switch shows that clients with the 802.1X supplicant are able to authenticate, but clients without the supplicant are not able to use web authentication. Which configuration option will correct this issue? A.&#160;&#160;&#160; switch(config)# aaa accounting auth-proxy default start-stop group radius B.&#160;&#160;&#160; switch(config-if)# authentication host-mode multi-auth C.&#160;&#160;&#160; switch(config-if)# webauth D.&#160;&#160;&#160; switch(config)# ip http server E.&#160;&#160;&#160; switch(config-if)# authentication priority webauth dot1x Answer: D QUESTION 28 Which option on the Cisco ASA appliance must be enabled when implementing botnet traffic filtering? A.&#160;&#160;&#160; HTTP inspection B.&#160;&#160;&#160; static entries in the botnet blacklist and whitelist C.&#160;&#160;&#160; global ACL D.&#160;&#160;&#160; NetFlow E.&#160;&#160;&#160; DNS inspection and DNS snooping Answer: E QUESTION 29 Which signature engine is used to create a custom IPS signature on a Cisco IPS appliance that triggers when a vulnerable web application identified by the "/runscript.php" URI is run? A.&#160;&#160;&#160; AIC HTTP B.&#160;&#160;&#160; Service HTTP C.&#160;&#160;&#160; String TCP D.&#160;&#160;&#160; Atomic IP E.&#160;&#160;&#160; META F.&#160;&#160;&#160; Multi-String Answer: B QUESTION 30 With the Cisco FlexVPN solution, which four VPN deployments are supported? (Choose four.) A.&#160;&#160;&#160; site-to-site IPsec tunnels? B.&#160;&#160;&#160; dynamic spoke-to-spoke IPSec tunnels? (partial mesh) C.&#160;&#160;&#160; remote access from software or hardware IPsec clients? D.&#160;&#160;&#160; distributed full mesh IPsec tunnels? E.&#160;&#160;&#160; IPsec group encryption using GDOI? F.&#160;&#160;&#160; hub-and-spoke IPsec tunnels? Answer: ABCF

http://www.passleader.com/350-018.html] QUESTION 31 Which four techniques can you use for IP management plane security? (Choose four.) A.&#160;&#160;&#160; Management Plane Protection B.&#160;&#160;&#160; uRPF C.&#160;&#160;&#160; strong passwords D.&#160;&#160;&#160; RBAC E.&#160;&#160;&#160; SNMP security measures F.&#160;&#160;&#160; MD5 authentication Answer: ACDE QUESTION 32 Which three statements about remotely triggered black hole filtering are true? (Choose three.) A.&#160;&#160;&#160; It filters undesirable traffic. B.&#160;&#160;&#160; It uses BGP or OSPF to trigger a network-wide remotely controlled response to attacks. C.&#160;&#160;&#160; It provides a rapid-response technique that can be used in handling security-related events and incidents. D.&#160;&#160;&#160; It requires uRPF. Answer: ACD QUESTION 33 Which three statements about Cisco Flexible NetFlow are true? (Choose three.) A.&#160;&#160;&#160; The packet information used to create flows is not configurable by the user. B.&#160;&#160;&#160; It supports IPv4 and IPv6 packet fields. C.&#160;&#160;&#160; It tracks all fields of an IPv4 header as well as sections of the data payload. D.&#160;&#160;&#160; It uses two types of flow cache, normal and permanent. E.&#160;&#160;&#160; It can be a useful tool in monitoring the network for attacks. Answer: BCE QUESTION 34 During a computer security forensic investigation, a laptop computer is retrieved that requires content analysis and information retrieval. Which file system is on it, assuming it has the default installation of Microsoft Windows Vista operating system? A.&#160;&#160;&#160; HSFS B.&#160;&#160;&#160; WinFS C.&#160;&#160;&#160; NTFS D.&#160;&#160;&#160; FAT E.&#160;&#160;&#160; FAT32 Answer: C QUESTION 35 Which three statements about the IANA are true? (Choose three.) A.&#160;&#160;&#160; IANA is a department that is operated by the IETF. B.&#160;&#160;&#160; IANA oversees global IP address allocation. C.&#160;&#160;&#160; IANA managed the root zone in the DNS. D.&#160;&#160;&#160; IANA is administered by the ICANN. E.&#160;&#160;&#160; IANA defines URI schemes for use on the Internet. Answer: BCD QUESTION 36 What does the Common Criteria (CC) standard define? A.&#160;&#160;&#160; The current list of Common Vulnerabilities and Exposures (CVEs) B.&#160;&#160;&#160; The U.S standards for encryption export regulations C.&#160;&#160;&#160; Tools to support the development of pivotal, forward-looking information system technologies D.&#160;&#160;&#160; The international standards for evaluating trust in information systems and products E.&#160;&#160;&#160; The international standards for privacy laws F.&#160;&#160;&#160; The standards for establishing a security incident response system Answer: D QUESTION 37 Which three types of information could be used during the incident response investigation phase? (Choose three.) A.&#160;&#160;&#160; netflow data B.&#160;&#160;&#160; SNMP alerts C.&#160;&#160;&#160; encryption policy D.&#160;&#160;&#160; syslog output E.&#160;&#160;&#160; IT compliance reports Answer: ABD QUESTION 38 Which of the following best describes Chain of Evidence in the context of security forensics? A.&#160;&#160;&#160; Evidence is locked down, but not necessarily authenticated. B.&#160;&#160;&#160; Evidence is controlled and accounted for to maintain its authenticity and integrity. C.&#160;&#160;&#160; The general whereabouts of evidence is known. D.&#160;&#160;&#160; Someone knows where the evidence is and can say who had it if it is not logged. Answer: B QUESTION 39 Which option is a benefit of implementing RFC 2827? A.&#160;&#160;&#160; prevents DoS from legitimate, non-hostile end systems B.&#160;&#160;&#160; prevents disruption of special services such as Mobile IP C.&#160;&#160;&#160; defeats DoS attacks which employ IP source address spoofing D.&#160;&#160;&#160; restricts directed broadcasts at the ingress router E.&#160;&#160;&#160; allows DHCP or BOOTP packets to reach the relay agents as appropriate Answer: C QUESTION 40 Which of the following provides the features of route summarization, assignment of contiguous blocks of addresses, and combining routes for multiple classful networks into a single route? A.&#160;&#160;&#160; classless interdomain routing B.&#160;&#160;&#160; route summarization C.&#160;&#160;&#160; supernetting D.&#160;&#160;&#160; private IP addressing Answer: A

PassLeader
Leader of IT Certifications

http://www.passleader.com/350-018.html]