

[Lead2pass New Free Downloading 400-251 Exam Dumps PDF From Lead2pass (326-350)]

2017 October Cisco Official New Released 400-251 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! We offer the most current and best training materials of the 400-251 certification Q&A , Practice Software, Study Packs, Preparation Labs and Audio Training you are looking for. Our online certification training offers you quick and cost-efficient way to train and become a certified professional in IT industry. Following questions and answers are all new published by Cisco Official Exam Center: <https://www.lead2pass.com/400-251.html>

QUESTION 326 What is the first step in performing a risk assessment? A. Identifying critical services and network vulnerabilities and determining the potential impact of their compromise or failure. B. Investigating reports of data theft or security breaches and assigning responsibility. C. Terminating any employee believed to be responsible for compromising security. D. Evaluating the effectiveness and appropriateness of the organization's current risk-management activities. E. Establishing a security team to perform forensic examinations of previous known attacks. Answer: A

QUESTION 327 What command can you use to display the number of malformed messages received by a DHCP server? A. show ip dhcp relay information trusted-sources B. show ip dhcp server statistics C. show ip dhcp conflict D. show ip dhcp binding E. show ip dhcp database Answer: B

QUESTION 328 Which of the following are two valid TLS message content types? (Choose two.) A. Alert B. Application data C. Proxy D. Identity E. Notification Dynamic F. Success Answer: AB

QUESTION 329 What are the two most common methods that security auditors use to assess an organization's security processes? (Choose two) A. social engineering attempts B. interviews C. policy assessment D. penetration testing E. document review F. Physical observation Answer: BF

Explanation: Check out the section called "Auditing security practices", namely the block for "Security process review": <http://www.ciscopress.com/articles/article.asp?p=1606900&seqNum=2>

QUESTION 330 All of these are available from Cisco IPS Device Manager (Cisco IDM) except which one? A. Top Signatures B. Sensor Information C. Interface Status D. Global Correlation Reports E. CPU, Memory and Load Answer: A

QUESTION 331 What SNMPv3 command disables descriptive error message? A. snmp-server trap link switchover B. snmp-server ifindex persist C. snmp-server inform D. snmp-server usm cisco Answer: D

QUESTION 332 Refer to the exhibit. Which line in the given configuration contains a locally significant value? A. tunnel key 123 B. ip nhrp authentication cisco C. ip nhrp map multicast 150.1.1.1 D. ip nhrp holdtime 60 E. ip nhrp network-id 123 Answer: E

QUESTION 333 What are the three flag bits in an IPv4 header? (Choose three.) A. TTL B. Unused C. Record Route D. DFE. MFF. Timestamp Answer: BDE

QUESTION 334 Which two parameters can the HostScan feature scan before users log on? (Choose two) A. whether specific files are present B. whether a proxy service is configured on a Linux host C. whether specific IPv4 and IPv6 addresses are assigned D. whether specific certificate authorities are configured E. whether a specific keychain entry exists on an OS X host Answer: AC

QUESTION 335 Refer to the exhibit. You have configured an NDAC seed switch as shown, but the switch is failing to allow other switches to securely join the domain. What command must you add to the seed switch's configuration to enable secure RADIUS communication? A. Seed-Switch(config)#radius.server host 10.1.1.2 auth-port 1812 acct-port 1813 test username ndac-test pac key Cisco123 B. Seed-Switch(config)#radius-server vsa send accounting C. Seed-Switch(config)#aaa preauth D. Seed-Switch(config)#no dot1x system-auth-control E. Seed-Switch(config)#radius-server host non-standard F. Seed-Switch(config)#aaa authentication dot1x default group local Answer: A

QUESTION 336 Refer to the exhibit. What is the effect of the given command? A. It enables CoPP on the FastEthernet 0/0 interface for SSH and SNMP management traffic. B. It enables MPP on the FastEthernet 0/0 interface for SSH and SNMP management traffic and CoPP for all other protocols. C. It enables MPP on the FastEthernet 0/0 interface, allowing only SSH and SNMP management traffic. D. It enables QoS policing on the control plane of the FastEthernet 0/0 interface. E. It enables MPP on the FastEthernet 0/0 interface by enforcing rate-limiting for SSH and SNMP management traffic. Answer: C

QUESTION 337 Which two statements about SCEP are true? (Choose two) A. CA servers must support GetCACaps response messages in order to implement extended functionality. B. The GetCRL exchange is signed and encrypted only in the response direction. C. It is vulnerable to downgrade attacks on its cryptographic capabilities. D. The GetCert exchange is signed and encrypted only in the response direction. E. The GetCACaps response message supports DES encryption and the SHA-128 hashing algorithm. Answer: AC

QUESTION 338 Which two events can cause a failover event on an active/standby setup? (Choose two.) A. The active unit experiences interface failure above the threshold. B. The unit that was previously active recovers. C. The stateful failover link fails. D. The failover link fails. E. The active unit fails Answer: AE

QUESTION 339 Which two statements about the MACsec security protocol are true? (Choose two.) A. Stations broadcast an MKA heartbeat that contains the key server priority. B. The SAK is secured by 128 bit AES-GCM by default. C. When switch-to-switch link security is configured in manual mode, the SAP operation mode must be set to GCMD. D. MACsec is not supported in MDA mode. E. MKA heartbeats

are sent at a default interval of 3 seconds. Answer: AB QUESTION 340 Which two options are benefits of network summarization? (Choose two.) A. It can summarize discontinuous IP addresses. B. It can easily be added to existing networks. C. It can increase the convergence of the network. D. It reduces the number of routes. E. It prevents unnecessary routing updates at the summarization boundary if one of the routes in the summary is unstable. Answer: DE QUESTION 341 Refer to the exhibit. Which meaning of this error message on a Cisco ASA is true? A. The route map redistribution is configured incorrectly. B. The default route is undefined. C. A packet was denied and dropped by an ACL. D. The host is connected directly to the firewall. Answer: B

QUESTION 342 Which two statements about uRPF are true? (Choose two.) A. The administrator can configure the allow-default command to force the routing table to use only the default route. B. It is not supported on the Cisco ASA security appliance. C. The administrator can configure the ip verify unicast source reachable-via any command to enable the RPF check to work routing groups. D. The administrator can use the show cef interface command to determine whether uRPF is enabled. E. In strict mode, only one routing path can be available to reach network devices on a subnet. Answer: AD QUESTION 343 Which type of header attack is detected by Cisco ASA basic threat detection? A. connection limit exceeded. B. denial by access list. C. failed application inspection. D. bad packet format. Answer: D QUESTION 344 Refer to the exhibit. A user authenticates to the NAS, which communicates to the TACACS+ server authentication. The TACACS+ SERVER then accesses the Active Directory Server through the ASA firewall to validate the user credentials. Which protocol-port pair must be allowed access through the ASA firewall? A. SMB over TCP 455. B. DNS over UDP 53. C. LDAP over UDP 389. D. global catalog over UDP 3268. E. TACACS+ over TCP 49. F. DNS over TCP 53. Answer: C QUESTION 345 Which WEP configuration can be exploited by a weak IV attack? A. When the static WEP password has been stored without encryption. B. When a per-packet WEP key is in use. C. When a 64-bit key is in use. D. When the static WEP password has been given away. E. When a 40-bit key is in use. F. When the same WEP key is used to create every pack. Answer: F QUESTION 346 Which two statements about Botnet Traffic Filter snooping are true? (Choose two.) A. It requires DNS packet inspection to be enabled to filter domain names in the dynamic database. B. It requires the Cisco ASA DNS server to perform DNS lookups. C. It can inspect both IPv4 and IPv6 traffic. D. It can log and block suspicious connections from previously unknown bad domains and IP addresses. E. It checks inbound traffic only. F. It checks inbound and outbound traffic. Answer: AF QUESTION 347 Which three statements about SXP are true? (Choose three.) A. It resides in the control plane, where connections can be initiated from a listener. B. Packets can be tagged with SGTs only with hardware support. C. Each VRF supports only one CTS-SXP connection. D. To enable an access device to use IP device tracking to learn source device IP addresses, DHCP snooping must be configured. E. The SGA ZBPF uses the SGT to apply forwarding decisions. F. Separate VRFs require different CTS-SXP peers, but they can use the same source IP addresses. Answer: BCE

QUESTION 348 Which file extensions are supported on the Firesight Management Center 3.1 file policies that can be analyzed dynamically using the Threat Grid Sandbox integration? A. MSEXE, MSOLE2, NEW-OFFICE, PDF, DOCX, WAV, XLS, TXT, TXTC, TXT, MSOLE2, WAV, PDF, DOC, MSOLE2, XML, PDF. Answer: A QUESTION 349 Refer to the exhibit. You applied this VPN cluster configuration to a Cisco ASA and the cluster failed to form. How do you edit the configuration to correct the problem? A. Define the maximum allowable number of VPN connections. B. Define the master/slave relationship. C. Configure the cluster IP address. D. Enable load balancing. Answer: C QUESTION 350 Which effect of the crypto pki authenticate command is true? A. It sets the certificate enrollment method. B. It retrieves and authenticates a CA certificate. C. It configures a CA trust point. D. It displays the current CA certificate. Answer: B

The strength of our 400-251 dumps is the constant update that we perform to keep abreast with the market trends and changes. Our 400-251 exam question is not only the best option for certification but also enhances your skill to an advance level. 400-251 new questions on Google Drive:

<https://drive.google.com/open?id=0B3Syig5i8gpDU1JrNmttR1dfUm8> 2017 Cisco 400-251 exam dumps (All 636 Q&As) from Lead2pass: <https://www.lead2pass.com/400-251.html> [100% Exam Pass Guaranteed]