[PDF&VCE Lead2pass Offering Free 300-207 Dumps Files For Free Downloading By 300-207 Exam Candidates (121-140)

 2016 October Cisco Official New Released 300-207 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! 2016 latest released Cisco official 300-207 exam question free download from Lead2pass! All new updated questions and answers are real questions from Cisco Exam Center! Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/300-207.html QUESTION 121 Refer to the exhibit. What Cisco ESA CLI command generated the output?

```
Status as of:              Wed May 22 16:05:13 2013 GMT
Hosts marked with '*' were down as of the last delivery attempt.

                          Active   Conn.    Deliv.     Soft      Hard
#    Recipient Host       Recip.   Out      Recip.   Bounced   Bounced

1    example.com            1       11       10078       0         1
2    acme.com               0        3       34021       0         0
3    biology.acme.com       0        9       64026       0         0
4    *chemistry.acme.com    0        2       94091       0         0
5    pluto.acme.com         0        6       75021       0         0
5    *venus.acme.com       100       0           0       0         0
7    the.encryption.queue   0        0       90649       0         0
8    the.euq.queue          0        0           1       0         0
9    the.euq.release.queue  0        0        4531       0         0

email.example.com>
```

    A.   smtproutes B.   tophosts C.   hoststatus D.   workqueuestatus Answer: B QUESTION 122 What Event Action in an IPS signature is used to stop an attacker from communicating with a network using an access-list? A.   Request Block Host B.   Deny Attacker Inline C.   Deny Connection Inline D.   Deny Packet Inline E.   Request Block Connection Answer: A QUESTION 123 Within Cisco IPS anomaly detection, what is the default IP range of the external zone? A.   0.0.0.0 0.0.0.0 B.   0.0.0.0 - 255.255.255.255 C.   0.0.0.0/8 D.   the network of the management interface Answer: B QUESTION 124 Which two Cisco IPS events will generate an IP log? (Choose two.) A.   A signature had an event action that was configured with log packets. B.   A statically configured IP or IP network criterion was matched. C.   A dynamically configured IP address or IP network was matched. D.   An attack produced a response action. Answer: AB QUESTION 125 Which three options are valid event actions for a Cisco IPS? (Choose three.) A.   deny-packet-inline B.   deny-attack-reset C.   produce-verbose-alert D.   log-attacker-packets E.   deny-packet-internal F.   request-block-drop-connection Answer: ACD QUESTION 126 Which configuration option causes an ASA with IPS module to drop traffic matching IPS signatures and to block all traffic if the module fails? A.   Inline Mode, Permit Traffic B.   Inline Mode, Close Traffic C.   Promiscuous Mode, Permit Traffic D.   Promiscuous Mode, Close Traffic Answer: B QUESTION 127 Which Cisco IPS CLI command shows the most fired signature? A.   show statistics virtual-sensor B.   show event alert C.   show alert D.   show version Answer: A QUESTION 128 Which IPS engine detects ARP spoofing? A.   Atomic ARP Engine B.   Service Generic Engine C.   ARP Inspection Engine D.   AIC Engine Answer: A QUESTION 129 Which two options are characteristics of router-based IPS? (Choose two.) A.   It supports custom signatures B.   It supports virtual sensors. C.   It supports multiple VRFs. D.   It uses configurable anomaly detection. E.   Signature definition files have been deprecated. Answer: CE QUESTION 130 An IPS is configured to fail-closed and you observe that all packets are dropped. What is a possible reason for this behavior? A.   Mainapp is unresponsive. B.   The global correlation update failed. C.   The IPS span session failed. D.   The attack drop file is misconfigured. Answer: A QUESTION 131 What can you use to access the Cisco IPS secure command and control channel to make configuration changes? A.   SDEE B.   the management interface C.   an HTTP server D.   Telnet Answer: B QUESTION 132 Which Cisco technology provides spam filtering and email protection? A.   IPS B.   ESA C.   WSA D.   CX Answer: B QUESTION 133 You ran the ssh generate-key command on the Cisco IPS and now administrators are unable to connect. Which action can be taken to correct the problem? A.   Replace the old key with a new key on the client. B.   Run the ssh host-key command. C.   Add the administrator IP addresses to the trusted TLS host list on the IPS. D.   Run the ssh authorized-keys command. Answer: A QUESTION 134 Which command allows the administrator to access the Cisco WSA on a secure channel on port 8443? A.   strictssl B.   adminaccessconfig C.   ssl D.   ssh Answer: A QUESTION 135 Which command can change the HTTPS SSL method on the Cisco ESA? A.   sslconfig B.   strictssl C.   sshconfig D.   adminaccessconfig Answer: A QUESTION 136 When you configure the Cisco ESA to perform blacklisting, what are two items you can disable to enhance performance?

(Choose two.) A.   spam scanning B.   antivirus scanning C.   APT detection D.   rootkit detection Answer: AB QUESTION 137 Which Cisco ESA predefined sender group uses parameter-matching to reject senders? A.   BLACKLIST B.   WHITELIST C. SUSPECTLIST D.   UNKNOWNLIST Answer: A QUESTION 138 Which command disables SSH access for administrators on the Cisco ESA? A.   interfaceconfig B.   sshconfig C.   sslconfig D.   systemsetup Answer: A QUESTION 139 When you create a new server profile on the Cisco ESA, which subcommand of the ldapconfig command configures spam quarantine end-user authentication? A.   isqauth B.   isqalias C.   test D.   server Answer: A QUESTION 140 Which three administrator actions are used to configure IP logging in Cisco IME? (Choose three.) A.   Select a virtual sensor. B.   Enable IP logging. C.   Specify the host IP address. D.   Set the logging duration. E.   Set the number of packets to capture. F.   Set the number of bytes to capture. Answer: ACD Lead2pass offers the latest Cisco 300-207 exam questions and answers in PDF & VCE. We promise 100% 300-207 exam pass or full money back (Have a try- If success, you will get a high pay job! Failed, nothing, money back!)! We provide instant download of our 300-207 dumps after payment so you can study earlier than others! 300-207 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDM2V5bnM0dTVhYjg 2016 Cisco 300-207 exam dumps (All 251 Q&As) from Lead2pass: http://www.lead2pass.com/300-207.html [100% Exam Pass Guaranteed]