[Lead2pass New Easily Pass NSE4 Exam By Training Lead2pass New Fortinet VCE Dumps (51-75)

2017 October Fortinet Official New Released NSE4 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!
Since I recently passed the the Fortinet NSE4 exam, it's time for me to share the Lead2pass exam dumps I used when preparing for this exam. Following questions and answers are all new published by Fortinet Official Exam Center: https://www.lead2pass.com/nse4.html QUESTION 51With FSSO, a domain user could authenticate either against the domain controller running the collector agent and domain controller agent, or a domain controller running only the domain controller agent. If you attempt to authenticate with a domain controller running only the domain controller agent, which statements are correct? (Choose two.) A. The login event is sent to the collector agent.B. The FortiGate receives the user information directly from the receiving domain controller agent of the secondary domain controller.C. The domain collector agent may perform a DNS lookup for the authenticated client's IP address.D. The user cannot be authenticated with the FortiGate in this manner because each domain controller agent requires a dedicated collector agent.Answer: AC QUESTION 52FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows active directory.Which of the following statements are correct regarding FSSO in a Windows domain environment when agent mode is used? (Choose two.) A. An FSSO collector agent must be installed on every domain controller.B. An FSSO domain controller agent must be installed on every domain controller.C. The FSSO domain controller agent will regularly update user logon information on the FortiGate unit.D. The FSSO collector agent will receive user logon information from the domain controller agent and will send it to the FortiGate unit. Answer: BD QUESTION 53Which statement is one disadvantage of using FSSO NetAPI polling mode over FSSO Security Event Log (WinSecLog) polling mode? A. It requires a DC agent installed in some of the Windows DC.B. It runs slower.C. It might miss some logon events.D. It requires access to a DNS server for workstation name resolution. Answer: C QUESTION 54Which are two requirements for DC-agent mode FSSO to work properly in a Windows AD environment? [Choose two.] A. DNS server must properly resolve all workstation names.B. The remote registry service must be running in all workstations.C. The collector agent must be installed in one of the Windows domain controllers.D. A same user cannot be logged in into two different workstations at the same time. Answer: AB QUESTION 55Which statement describes what the CLI command diagnose debug authd fsso list is used for? A. Monitors communications between the FSSO collector agent and FortiGate unit.B. Displays which users are currently logged on using FSSO.C. Displays a listing of all connected FSSO collector agents.D. Lists all DC Agents installed on all domain controllers. Answer: B QUESTION 56When the SSL proxy is NOT doing man-in-the-middle interception of SSL traffic, which certificate field can be used to determine the rating of a website? A. Organizational Unit.B. Common Name. C. Serial Number.D. Validity. Answer: B QUESTION 57Which tasks fall under the responsibility of the SSL proxy in a typical HTTPS connection? (Choose two.) A. The web client SSL handshake.B. The web server SSL handshake.C. File buffering.D. Communication with the URL filter process. Answer: AB QUESTION 58Bob wants to send Alice a file that is encrypted using public key cryptography.Which of the following statements is correct regarding the use of public key cryptography in this scenario? A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.B. Bob will use his public key to encrypt the file and Alice will use Bob's private key to decrypt the file.C. Bob will use Alice's public key to encrypt the file and Alice will use her private key to decrypt the file.D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the file. Answer: C QUESTION 59Which Fortinet products & features could be considered part of a comprehensive solution to monitor and prevent the leakage of senstive data? (Select all that apply.) A. Archive non-compliant outgoing e-mails using FortiMail.B. Restrict unofficial methods of transferring files such as P2P using Application Control lists on a FortiGate.C. Monitor database activity using FortiAnalyzer.D. Apply a DLP sensor to a firewall policy.E. Configure FortiClient to prevent files flagged as sensitive from being copied to a USB disk. Answer: ABD QUESTION 60For data leak prevention, which statement describes the difference between the block and quarantine actions? A. A block action prevents the transaction. A quarantine action blocks all future transactions, regardless of the protocol.B. A block action prevents the transaction. A quarantine action archives the data.C. A block action has a finite duration. A quarantine action must be removed by an administrator.D. A block action is used for known users. A quarantine action is used for unknown users. Answer: A QUESTION 61In which process states is it impossible to interrupt/kill a process? (Choose two.) A. S - SleepB. R - RunningC. D - Uninterruptable SleepD. Z - Zombie Answer: CD QUESTION 62Examine at the output below from the diagnose sys top command: # diagnose sys top 1Run Time: 11 days, 3 hours and 29 minutes0U, 0N, 1S, 99I; 971T, 528F, 160KFsshd 123 S 1.9 1.2 ipsengine 61 S < 0.0 5.2miglogd 45 S 0.0 4.9pyfcgid 75 S 0.0 4.5pyfcgid 73 S 0.0 3.9 Which statements are true regarding the output above? (Choose two.) A. The sshd process is the one consuming most CPU.B. The sshd process is using 123 pages of

memory.C. The command diagnose sys kill miglogd will restart the miglogd process.D. All the processes listed are in sleeping state. Answer: AD QUESTION 63Examine the following output from the diagnose sys session list command: session info: proto=6 proto_state=65 duration=3 expire=9 timeout=3600 flags=00000000 sockflag=00000000 sockport=443 av_idx=9 use=5 origin-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps reply-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bpsstate=redir local may_dirty ndr npu nlb os rsstatistic(bytes/packets/allow_err): org=864/8/1 reply=2384/7/1 tuples=3orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.17.87.3/10.1.10.1hook=post dir=org act=snat 192.168.1.110:57999->74.201.86.29:443(172.17.87.16:57999)hook=pre dir=reply act=dnat 74.201.86.29:443->172.17.87.16:57999(192.168.1.110:57999)hook=post dir=reply act=noop 74.201.86.29:443->192.168.1.110:57999(0.0.0.0:0) misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0/0 Which statements are true regarding the session above? (Choose two.) A. Session Time-To-Live (TTL) was configured to 9 seconds.B. FortiGate is doing NAT of both the source and destination IP addresses on all packets coming from the 192.168.1.110 address.C. The IP address 192.168.1.110 is being translated to 172.17.87.16.D. The FortiGate is not translating the TCP port numbers of the packets in this session. Answer: CD QUESTION 64Which statements are correct regarding an IPv6 over IPv4 IPsec configuration? (Choose two.) A. The source quick mode selector must be an IPv4 address.B. The destination quick mode selector must be an IPv6 address.C. The Local Gateway IP must be an IPv4 address.D. The remote gateway IP must be an IPv6 address. Answer: BC QUESTION 65Which statements are true regarding IPv6 anycast addresses? (Choose two.) A. Multiple interfaces can share the same anycast address.B. They are allocated from the multicast address space.C. Different nodes cannot share the same anycast address.D. An anycast packet is routed to the nearest interface. Answer: AD QUESTION 66What functions can the IPv6 Neighbor Discovery protocol accomplish? (Choose two.) A. Negotiate the encryption parameters to use.B. Auto-adjust the MTU setting.C. Autoconfigure addresses and prefixes.D. Determine other nodes reachability. Answer: CD QUESTION 67Which is one of the conditions that must be met for offloading the encryption and decryption of IPsec traffic to an NP6 processor? A. No protection profile can be applied over the IPsec traffic.B. Phase-2 anti-replay must be disabled.C. Both the phase 1 and phases 2 must use encryption algorithms supported by the NP6.D. IPsec traffic must not be inspected by any FortiGate session helper. Answer: C QUESTION 68Which statements are true about offloading antivirus inspection to a Security Processor (SP)? (Choose two.) A. Both proxy-based and flow-based inspection are supported.B. A replacement message cannot be presented to users when a virus has been detected.C. It saves CPU resources.D. The ingress and egress interfaces can be in different SPs. Answer: BC QUESTION 69Which IP packets can be hardware-accelerated by a NP6 processor? (Choose two.) A. Fragmented packet.B. Multicast packet.C. SCTP packet.D. GRE packet. Answer: BC QUESTION 70Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic. What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.) A. They are accelerated by hardware in the master unit.B. They are not accelerated by hardware in the master unit.C. They are accelerated by hardware in the slave unit.D. They are not accelerated by hardware in the slave unit. Answer: AD QUESTION 71How is the FortiGate password recovery process? A. Interrupt boot sequence, modify the boot registry and reboot. After changing the password, reset the boot registry.B. Log in through the console port using the "maintainer" account within several seconds of physically power cycling the FortiGate.C. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.D. Interrupt the boot sequence and restore a configuration file for which the password has been modified. Answer: B QUESTION 72What are valid options for handling DNS requests sent directly to a FortiGates interface IP? (Choose three.) A. Conditional-forward.B. Forward-only.C. Non-recursive.D. Iterative.E. Recursive. Answer: BCE QUESTION 73When creating FortiGate administrative users, which configuration objects specify the account rights? A. Remote access profiles.B. User groups.C. Administrator profiles.D. Local-in policies. Answer: C QUESTION 74Which statements are true regarding the factory default configuration? (Choose three.) A. The default web filtering profile is applied to the first firewall policy.B. The `Port1' or `Internal' interface has the IP address 192.168.1.99.C. The implicit firewall policy action is ACCEPT.D. The `Port1' or `Internal' interface has a DHCP server set up and enabled (on device models that support DHCP servers).E. Default login uses the username: admin (all lowercase) and no password. Answer: BDE QUESTION 75What methods can be used to access the FortiGate CLI? (Choose two.) A. Using SNMP.B. A direct connection to the serial console port.C. Using the CLI console widget in the GUI.D. Using RCP. Answer: BC I hope Lead2pass exam questions from the Fortinet NSE4 exam helps you pass the exam and earn your Fortinet certification! Happy Studying! NSE4 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDeFZLNEJDeDRQdlE 2017 Fortinet **NSE4** exam dumps (All 533 Q&As) from Lead2pass: https://www.lead2pass.com/nse4.html [100% Exam Pass Guaranteed]