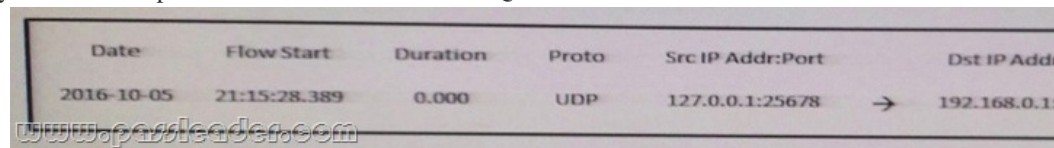


[Feb-2017 Dumps All People Wanted! PassLeader Valid 70q 210-255 Exam Questions For Free Download

New Updated 210-255 Exam Questions from PassLeader 210-255 PDF dumps! Welcome to download the newest PassLeader 210-255 VCE dumps: <http://www.passleader.com/210-255.html> (70 Q&As) Keywords: 210-255 exam dumps, 210-255 exam questions, 210-255 VCE dumps, 210-255 PDF dumps, 210-255 practice tests, 210-255 study guide, 210-255 braindumps, Implementing Cisco Cybersecurity Operations Exam P.S. Free 210-255 dumps download from Google Drive: https://drive.google.com/open?id=0B-ob6L_QjGLpNjM1MWNkbHM5OW8 **NEW QUESTION 1** Which option can be addressed when using retrospective security techniques? A. if the affected host needs a software update B. how the malware entered our network C. why the malware is still in our network D. if the affected system needs replacement **Answer: A** **NEW QUESTION 2** Refer to the exhibit. Which type of log is this an example of?



Date	Flow Start	Duration	Proto	Src IP Addr:Port	Dst IP Addr
2016-10-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→ 192.168.0.1

A. IDS log B. proxy log C. NetFlow log D. syslog **Answer: A** **NEW QUESTION 3** Which option is a misuse variety per VERIS enumerations? A. snooping B. hacking C. theft D. assault **Answer: B** **NEW QUESTION 4** In the context of incident handling phases, which two activities fall under scoping? (Choose two.) A. determining the number of attackers that are associated with a security incident B. ascertaining the number and types of vulnerabilities on your network C. identifying the extent that a security incident is impacting protected resources on the network D. determining what and how much data may have been affected E. identifying the attackers that are associated with a security incident **Answer: DE** **NEW QUESTION 5** Which regular expression matches "color" and "colour"? A. col[0-9]+our B. colo?ur C. colour?r D. [a-z]{7} **Answer: C** **NEW QUESTION 6** Which component of the NIST SP800-61 r2 incident handling strategy reviews data? A. preparation B. detection and analysis C. containment, eradication, and recovery D. post-incident analysis **Answer: B** **NEW QUESTION 7** Which option is generated when a file is run through an algorithm and generates a string specific to the contents of that file? A. URL B. hash C. IP address D. destination port **Answer: C** **NEW QUESTION 8** Which data type is protected under the PCI compliance framework? A. credit card type B. primary account number C. health conditions D. provision of individual care **Answer: C** **NEW QUESTION 9** Which kind of evidence can be considered most reliable to arrive at an analytical assertion? A. direct B. corroborative C. indirect D. circumstantial E. textual **Answer: A** **NEW QUESTION 10** ?? Download the newest PassLeader 210-255 dumps from passleader.com now! 100% Pass Guarantee! 210-255 PDF dumps & 210-255 VCE dumps: <http://www.passleader.com/210-255.html> (70 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. Free 210-255 Exam Dumps Collection On Google Drive: https://drive.google.com/open?id=0B-ob6L_QjGLpNjM1MWNkbHM5OW8