[2017 New Lead2pass Latest SY0-401 Free Dumps Guarantee SY0-401 Certification Exam 100% Success (151-175)

2017 August CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!
Lead2pass updates CompTIA SY0-401 exam questions, adds some new changed questions from CompTIA Official Exam Center. Want to know 2017 SY0-401 exam test points? Download the following free Lead2pass latest exam questions today! Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html
QUESTION 151Drag and Drop QuestionsDrag and drop the correct protocol to its default port. Answer: Explanation:When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.
QUESTION 152Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools? A. Identify user habitsB. Disconnect system from networkC. Capture system imageD. Interview witnesses Answer: C Explanation:Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. Very much as helpful in same way that a virus sample is kept in laboratories to study later after a breakout. Also you should act in the order of volatility which states that the system image capture is first on the list of a forensic analysis.
QUESTION 153Computer evidence at a crime is preserved by making an exact copy of the hard disk. Which of the following does this illustrate? A. Taking screenshotsB. System image captureC. Chain of custodyD. Order of volatility Answer: B Explanation:A system image would be a snapshot of what exists at the moment. Thus capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. QUESTION 154To ensure proper evidence collection, which of the following steps should be performed FIRST? A. Take hashes from the live systemB. Review logsC. Capture the system imageD. Copy all compromised files Answer: CExplanation:Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. This is essential since the collection of evidence process may result in some mishandling and changing the exploited state. QUESTION 155A security administrator needs to image a large hard drive for forensic analysis. Which of the following will allow for faster imaging to a second hard drive? A. cp /dev/sda /dev/sdb bs=8kB. tail -f /dev/sda > /dev/sdb bs=8kC. dd in=/dev/sda out=/dev/sdb bs=4kD. locate /dev/sda /dev/sdb bs=4k Answer: CExplanation:dd is a command-line utility for Unix and Unix-like operating systems whose primary purpose is to convert and copy files. dd can duplicate data across files, devices, partitions and volumes On Unix, device drivers for hardware (such as hard disks) and special device files (such as /dev/zero and /dev/random) appear in the file system just like normal files; dd can also read and/or write from/to these files, provided that function is implemented in their respective driver. As a result, dd can be used for tasks such as backing up the boot sector of a hard drive, and obtaining a fixed amount of random data. The dd program can also perform conversions on the data as it is copied, including byte order swapping and conversion to and from the ASCII and EBCDIC text encodings.An attempt to copy the entire disk using cp may omit the final block if it is of an unexpected length; whereas dd may succeed. The source and destination disks should have the same size. QUESTION 156A security technician wishes to gather and analyze all Web traffic during a particular time period.Which of the following represents the BEST approach to gathering the required data? A. Configure a VPN concentrator to log all traffic destined for ports 80 and 443.B. Configure a proxy server to log all traffic destined for ports 80 and 443.C. Configure a switch to log all traffic destined for ports 80 and 443.D. Configure a NIDS to log all traffic destined for ports 80 and 443. Answer: BExplanation:A proxy server is in essence a device that acts on behalf of others and in security terms all internal user interaction with the Internet should be controlled through a proxy server. This makes a proxy server the best tool to gather the required data. QUESTION 157A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site were facing the wrong direction to capture the incident. The analyst ensures the cameras are turned to face the proper direction. Which of the following types of controls is being used? A. DetectiveB. DeterrentC. CorrectiveD. Preventive Answer: CExplanation:A corrective control would be any corrective action taken to correct any existing control that were faulty or wrongly installed ?as in this case the cameras were already there, it just had to be adjusted to perform its function as intended. QUESTION 158Joe, a security administrator, is concerned with users tailgating into the restricted areas. Given a limited budget, which of the following would BEST assist Joe with detecting this activity? A. Place a full-time guard at the entrance to confirm user identity.B. Install a camera and DVR at the entrance to monitor access.C. Revoke

all proximity badge access to make users justify access.D. Install a motion detector near the entrance. Answer: BExplanation: Tailgating is a favorite method of gaining entry to electronically locked systems by following someone through the door they just unlocked. With a limited budget installing a camera and DVR at the entrance to monitor access to the restricted areas is the most feasible solution. The benefit of a camera (also known as closed-circuit television, or CCTV) is that it is always running and can record everything it sees, creating evidence that can be admissible in court if necessary. QUESTION 159The incident response team has received the following email message. From: monitor@ext-company.comTo: security@company.comSubject: Copyright infringement A copyright infringement alert was triggered by IP address 13.10.66.5 at 09: 50: 01 GMT.After reviewing the following web logs for IP 13.10.66.5, the team is unable to correlate and identify the incident. 09: 45: 33 13.10.66.5 http: //remote.site.com/login.asp?user=john09: 50: 22 13.10.66.5 http: //remote.site.com/logout.asp?user=anne10: 50: 01 13.10.66.5 http: //remote.site.com/access.asp?file=movie.mov11: 02: 45 13.10.65.5 http: //remote.site.com/download.asp?movie.mov=ok Which of the following is the MOST likely reason why the incident response team is unable to identify and correlate the incident? A. The logs are corrupt and no longer forensically sound.B. Traffic logs for the incident are unavailable.C. Chain of custody was not properly maintained.D. Incident time offsets were not accounted for. Answer: DExplanation:It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system. QUESTION 160A system administrator is responding to a legal order to turn over all logs from all company servers. The system administrator records the system time of all servers to ensure that: A. HDD hashes are accurate.B. the NTP server works properly.C. chain of custody is preserved.D. time offset can be calculated. Answer: DExplanation:It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system. QUESTION 161A recent intrusion has resulted in the need to perform incident response procedures. The incident response team has identified audit logs throughout the network and organizational systems which hold details of the security breach. Prior to this incident, a security consultant informed the company that they needed to implement an NTP server on the network. Which of the following is a problem that the incident response team will likely encounter during their assessment? A. Chain of custodyB. Tracking man hoursC. Record time offsetD. Capture video traffic Answer: CExplanation:It is quite common for workstation as well as server times to be off slightly from actual time. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system. There is no mention that this was done by the incident response team. QUESTION 162Computer evidence at a crime scene is documented with a tag stating who had possession of the evidence at a given time.Which of the following does this illustrate? A. System image captureB. Record time offsetC. Order of volatilityD. Chain of custody Answer: DExplanation:Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. QUESTION 163A compromised workstation utilized in a Distributed Denial of Service (DDOS) attack has been removed from the network and an image of the hard drive has been created. However, the system administrator stated that the system was left unattended for several hours before the image was created. In the event of a court case, which of the following is likely to be an issue with this incident? A. Eye WitnessB. Data Analysis of the hard driveC. Chain of custodyD. Expert Witness Answer: CExplanation:Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. The evidence must always be within your custody, or you're open to dispute about possible evidence tampering. QUESTION 164The security manager received a report that an employee was involved in illegal activity and has saved data to a workstation's hard drive. During the investigation, local law enforcement's criminal division confiscates the hard drive as evidence. Which of the following forensic procedures is involved? A. Chain of custodyB. System imageC. Take hashesD. Order of volatility Answer: AExplanation:Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. QUESTION 165Which of the following is the MOST important step for preserving evidence during

forensic procedures? A. Involve law enforcementB. Chain of custodyC. Record the time of the incidentD. Report within one hour of discovery Answer: BExplanation:Chain of custody deals with how evidence is secured, where it is stored, and who has access to it.When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. The evidence must always be within your custody, or you're open to dispute about possible evidence tampering. Thus to preserve evidence during a forensic procedure the chain of custody is of utmost importance. QUESTION 166 During which of the following phases of the Incident Response process should a security administrator define and implement general defense against malware? A. Lessons LearnedB. PreparationC. EradicationD. Identification Answer: BExplanation: Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. It is important to stop malware before it ever gets hold of a system thus you should know which malware is out there and take defensive measures - this means preparation to guard against malware infection should be done. QUESTION 167The Chief Technical Officer (CTO) has tasked The Computer Emergency Response Team (CERT) to develop and update all Internal Operating Procedures and Standard Operating Procedures documentation in order to successfully respond to future incidents. Which of the following stages of the Incident Handling process is the team working on? A. Lessons LearnedB. EradicationC. RecoveryD. Preparation Answer: DExplanation:Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Developing and updating all internal operating and standard operating procedures documentation to handle future incidents is preparation. QUESTION 168The helpdesk reports increased calls from clients reporting spikes in malware infections on their systems. Which of the following phases of incident response is MOST appropriate as a FIRST response? A. RecoveryB. Follow-upC. ValidationD. IdentificationE. EradicationF. Containment Answer: DExplanation:To be able to respond to the incident of malware infection you need to know what type of malware was used since there are many types of malware around. This makes identification critical in this case. QUESTION 169Who should be contacted FIRST in the event of a security breach? A. Forensics analysis teamB. Internal auditorsC. Incident response teamD. Software vendors Answer: CExplanation:A security breach is an incident and requires a response. The incident response team would be better equipped to deal with any incident insofar as all their procedures are concerned. Their procedures in addressing incidents are: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. QUESTION 170In which of the following steps of incident response does a team analyse the incident and determine steps to prevent a future occurrence? A. MitigationB. IdentificationC. PreparationD. Lessons learned Answer: DExplanation:Incident response procedures involves in chronological order: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Thus lessons are only learned after the mitigation occurred. For only then can you `step back' and analyze the incident to prevent the same occurrence in future. QUESTION 171After a recent security breach, the network administrator has been tasked to update and backup all router and switch configurations. The security administrator has been tasked to enforce stricter security policies. All users were forced to undergo additional user awareness training. All of these actions are due to which of the following types of risk mitigation strategies? A. Change managementB. Implementing policies to prevent data lossC. User rights and permissions reviewD. Lessons learned Answer: DExplanation:Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Described in the question is a situation where a security breach had occurred and its response which shows that lessons have been learned and used to put in place measures that will prevent any future security breaches of the same kind. QUESTION 172A server dedicated to the storage and processing of sensitive information was compromised with a rootkit and sensitive data was extracted. Which of the following incident response procedures is best suited to restore the server? A. Wipe the storage, reinstall the OS from original media and restore the data from the last known good backup. B. Keep the data partition, restore the OS from the most current backup and run a full system antivirus scan.C. Format the storage and reinstall both the OS and the data from the most current backup.D. Erase the storage, reinstall the OS from most current backup and only restore the data that was not compromised. Answer: AExplanation:Rootkits are software programs that have the ability to hide certain things from the operating system. With a rootkit, there may be a number of processes running on a system that do not show up in Task Manager or connections established or available that do not appear in a netstat display--the rootkit masks the presence of these items. The rootkit is able to do this by manipulating function calls to the operating system and filtering

out information that would normally appear. Theoretically, rootkits could hide anywhere that there is enough memory to reside: video cards, PCI cards, and the like. The best way to handle this situation is to wipe the server and reinstall the operating system with the original installation disks and then restore the extracted data from your last known good backup. This way you can eradicate the rootkit and restore the data. QUESTION 173In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in question from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO). A. Take hashesB. Begin the chain of custody paperworkC. Take screen shotsD. Capture the system imageE. Decompile suspicious files Answer: ADExplanation:A: Take Hashes. NIST (the National Institute of Standards and Technology) maintains a National Software Reference Library (NSRL). One of the purposes of the NSRL is to collect "known, traceable software applications" through their hash values and store them in a Reference Data Set (RDS). The RDS can then be used by law enforcement, government agencies, and businesses to determine which fi les are important as evidence in criminal investigations.D: A system image is a snapshot of what exists. Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. QUESTION 174Which of the following is the LEAST volatile when performing incident response procedures? A. RegistersB. RAID cacheC. RAMD. Hard drive Answer: DExplanation:An example of OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts. Of the options stated in the question the hard drive would be the least volatile. QUESTION 175The security officer is preparing a read-only USB stick with a document of important personal phone numbers, vendor contacts, an MD5 program, and other tools to provide to employees. At which of the following points in an incident should the officer instruct employees to use this information? A. Business Impact AnalysisB. First ResponderC. Damage and Loss ControlD. Contingency Planning Answer: BExplanation: Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. In this scenario the security officer is carrying out an incident response measure that will address and be of benefit to those in the vanguard, i.e. the employees and they are the first responders. Lead2pass promise that all SY0-401 exam questions are the latest updated, we aim to provide latest and guaranteed questions for all certifications. You just need to be braved in trying then we will help you arrange all later things! 100% pass all exams you want or full money back! Do you want to have a try on passing SY0-401? SY0-401 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDVzFZWExUbFM0YU0 2017 CompTIA **SY0-401** exam dumps (All 1868 Q&As) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]