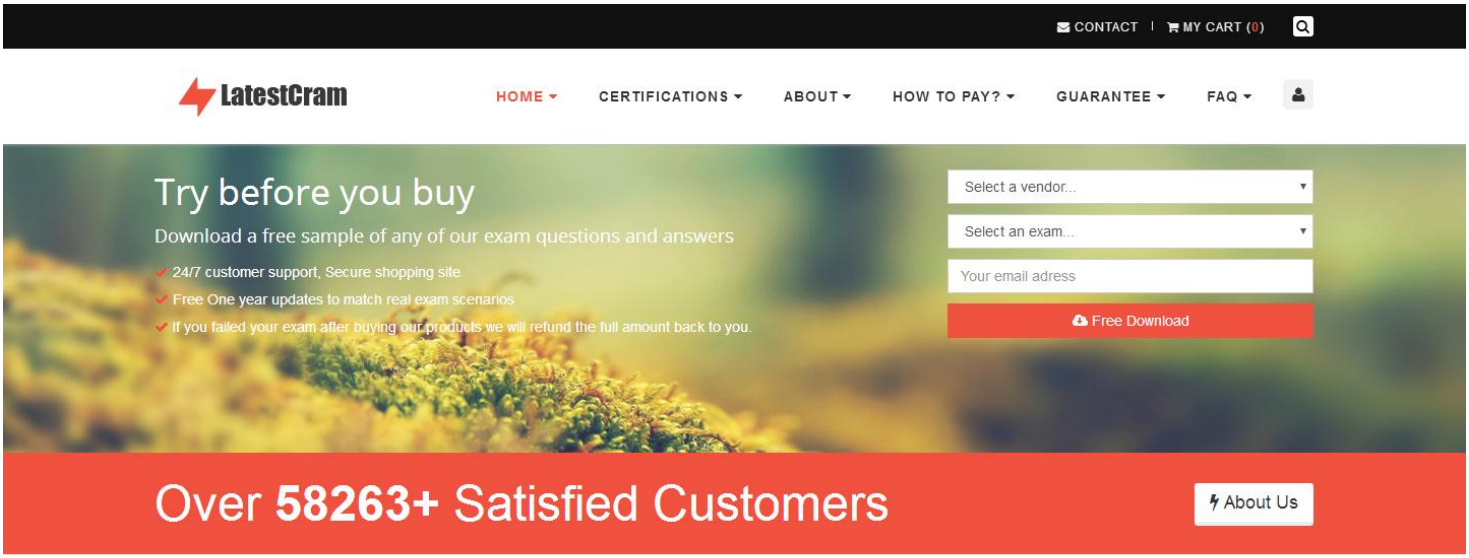
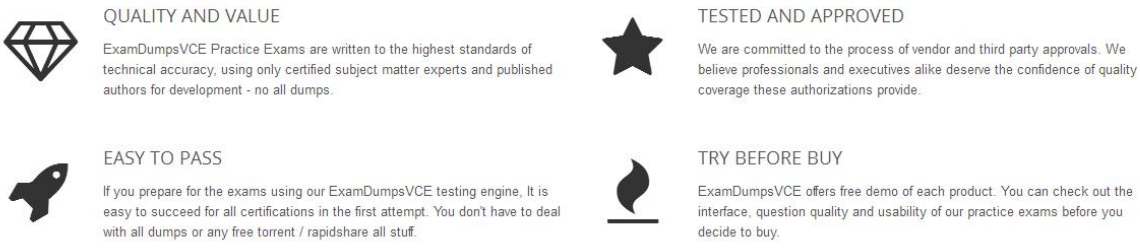
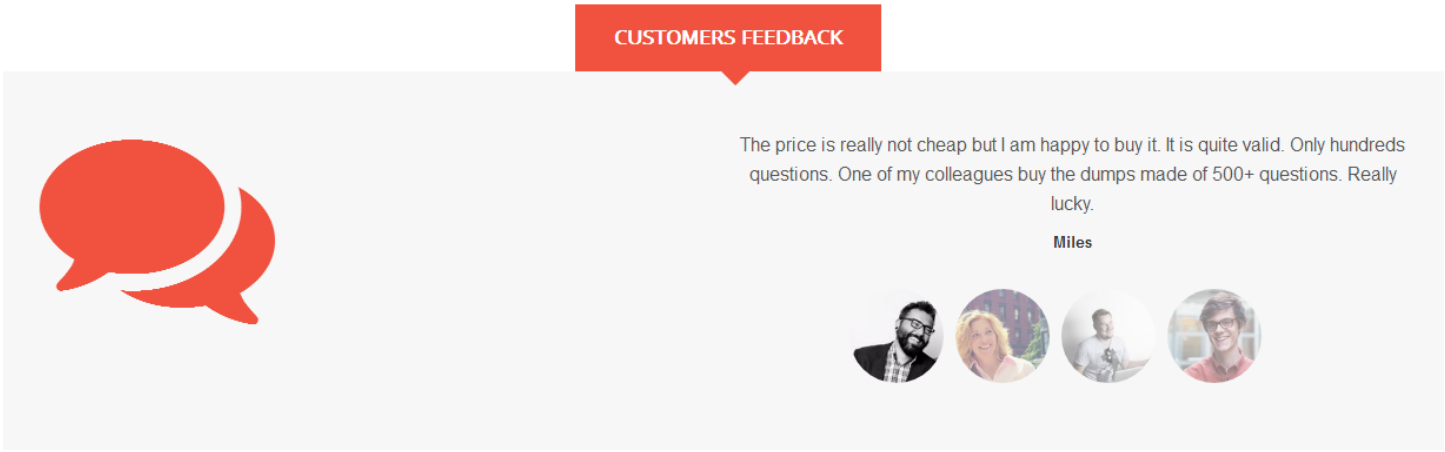
LatestCram

LatestCram







http://www.latestcram.com

Reliable Exam Braindumps & Valid Latest Questions & Right Exam Cram

Exam : **CAS-001**

Title : CompTIA Advanced Security Practitioner

Vendor : CompTIA

Version : DEMO

NO.1 Company Z is merging with Company A to expand its global presence and consumer base. This purchase includes several offices in different countries. To maintain strict internal security and compliance requirements, all employee activity may be monitored and reviewed. Which of the following would be the MOST likely cause for a change in this practice?
A. The excessive time it will take to merge the company's information systems.
B. Countries may have different legal or regulatory requirements.
C. Company A might not have adequate staffing to conduct these reviews.
D. The companies must consolidate security policies during the merger.
Answer: B

NO.2 An organization has had component integration related vulnerabilities exploited in consecutive releases of the software it hosts. The only reason the company was able to identify the compromises was because of a correlation of slow server performance and an attentive security analyst noticing unusual outbound network activity from the application servers. End-to-end management of the development process is the responsibility of the applications development manager and testing is done by various teams of programmers. Which of the following will MOST likely reduce the likelihood of similar incidents?
A. Conduct monthly audits to verify that application modifications do not introduce new vulnerabilities.
B. Implement a peer code review requirement prior to releasing code into production.
C. Follow secure coding practices to minimize the likelihood of creating vulnerable applications.
D. Establish cross-functional planning and testing requirements for software development activities.
Answer: D

NO.3 A new IDS device is generating a very large number of irrelevant events. Which of the following would BEST remedy this problem?
A. Change the IDS to use a heuristic anomaly filter.
B. Adjust IDS filters to decrease the number of false positives.
C. Change the IDS filter to data mine the false positives for statistical trending data.
D. Adjust IDS filters to increase the number of false negatives.
Answer: B

NO.4 The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router's external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company's external router's IP which is 128.20.176.19:
11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400
Which of the following describes the findings the senior security engineer should report to the ISO and the BEST solution for service restoration?
A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company's ISP should be contacted and instructed to block the malicious packets.
B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.
C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGP sinkhole should be configured to drop traffic at the source networks.
D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company's external router to block incoming UDP port 19 traffic.
Answer: A

NO.5 A company data center provides Internet based access to email and web services.
The firewall is separated into four zones:
-RED ZONE is an Internet zone -ORANGE ZONE a Web DMZ -YELLOW ZONE an email DMZ -GREEN ZONE is a management interface There are 15 email servers and 10 web servers. The data center administrator plugs a laptop into the management interface to make firewall changes. The administrator would like to secure this environment but has a limited budget. Assuming each addition is an appliance, which of the following would provide the MOST appropriate placement of security solutions while minimizing the expenses?
A. RED ZONE: none ORANGE ZONE: WAF YELLOW ZONE: SPAM Filter GREEN ZONE: none
B. RED ZONE: Virus Scanner, SPAM Filter ORANGE ZONE: NIPS YELLOW ZONE: NIPS GREEN ZONE: NIPS
C. RED ZONE: WAF, Virus Scanner ORANGE ZONE: NIPS YELLOW ZONE: NIPS GREEN ZONE: SPAM Filter
D. RED ZONE: NIPS ORANGE ZONE: WAF YELLOW ZONE: Virus Scanner, SPAM Filter GREEN ZONE: none
Answer: D

NO.6 A company's security policy states that its own internally developed proprietary Internet facing software must be resistant to web application attacks. Which of the following methods provides the MOST protection against unauthorized access to stored database information?
A. Require all development to follow secure coding practices.
B. Require client-side input filtering on all modifiable fields.
C. Escape character sequences at the application tier.
D. Deploy a WAF with application specific signatures.
Answer: A

NO.7 A large organization has recently suffered a massive credit card breach. During the months of Incident Response, there were multiple attempts to assign blame as to whose fault it was that the incident occurred. In which part of the incident response phase would this be addressed in a controlled and productive manner?

A. During the Identification Phase
B. During the Lessons Learned phase
C. During the Containment Phase
D. During the Preparation Phase
Answer: B

NO.8 A company receives an e-discovery request for the Chief Information Officer's (CIO's) email data. The storage administrator reports that the data retention policy relevant to their industry only requires one year of email data. However the storage administrator also reports that there are three years of email data on the server and five years of email data on backup tapes. How many years of data MUST the company legally provide?
A. 1
B. 2
C. 3
D. 5
Answer: D

NO.9 As part of a new wireless implementation, the Chief Information Officer's (CIO's) main objective is to immediately deploy a system that supports the 802.11r standard, which will help wireless VoIP devices in moving vehicles. However, the 802.11r standard was not ratified by the IETF. The wireless vendor's products do support the pre-ratification version of 802.11r. The security and network administrators have tested the product and do not see any security or compatibility issues; however, they are concerned that the standard is not yet final. Which of the following is the BEST way to proceed?
A. Purchase the equipment now, but do not use 802.11r until the standard is ratified.
B. Do not purchase the equipment now as the client devices do not yet support 802.11r.
C. Purchase the equipment now, as long as it will be firmware upgradeable to the final 802.11r standard.
D. Do not purchase the equipment now; delay the implementation until the IETF has ratified the final 802.11r standard.
Answer: C

NO.10 A security administrator was doing a packet capture and noticed a system communicating with an address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network. Which of the following is the BEST course of action?
A. Investigate the network traffic and block UDP port 3544 at the firewall
B. Remove the system from the network and disable IPv6 at the router
C. Locate and remove the unauthorized 6to4 relay from the network
D. Disable the switch port and block the 2001::/32 traffic at the firewall
Answer: A

NO.11 A manager who was attending an all-day training session was overdue entering bonus and payroll information for subordinates. The manager felt the best way to get the changes entered while

in training was to log into the payroll system, and then activate desktop sharing with a trusted subordinate. The manager granted the subordinate control of the desktop thereby giving the subordinate full access to the payroll system. The subordinate did not have authorization to be in the payroll system. Another employee reported the incident to the security team. Which of the following would be the MOST appropriate method for dealing with this issue going forward?
A. Provide targeted security awareness training and impose termination for repeat violators.
B. Block desktop sharing and web conferencing applications and enable use only with approval.
C. Actively monitor the data traffic for each employee using desktop sharing or web conferencing applications.
D. Permanently block desktop sharing and web conferencing applications and do not allow its use at the company.
Answer: A

NO.12 A company has been purchased by another agency and the new security architect has identified new security goals for the organization. The current location has video surveillance throughout the building and entryways. The following requirements must be met:
1.Ability to log entry of all employees in and out of specific areas
2.Access control into and out of all sensitive areas
3.Two-factor authentication
Which of the following would MOST likely be implemented to meet the above requirements and provide a secure solution? (Select TWO).
A. Proximity readers
B. Visitor logs
C. Biometric readers
D. Motion detection sensors
E. Mantrap
Answer: A,C

NO.13 A wholesaler has decided to increase revenue streams by selling direct to the public through an on-line system. Initially this will be run as a short term trial and if profitable, will be expanded and form part of the day to day business. The risk manager has raised two main business risks for the initial trial:
1.IT staff has no experience with establishing and managing secure on-line credit card processing.
2.An internal credit card processing system will expose the business to additional compliance requirements.
Which of the following is the BEST risk mitigation strategy?
A. Transfer the risks to another internal department, who have more resources to accept the risk.
B. Accept the risks and log acceptance in the risk register. Once the risks have been accepted close them out.
C. Transfer the initial risks by outsourcing payment processing to a third party service provider.
D. Mitigate the risks by hiring additional IT staff with the appropriate experience and certifications.
Answer: C

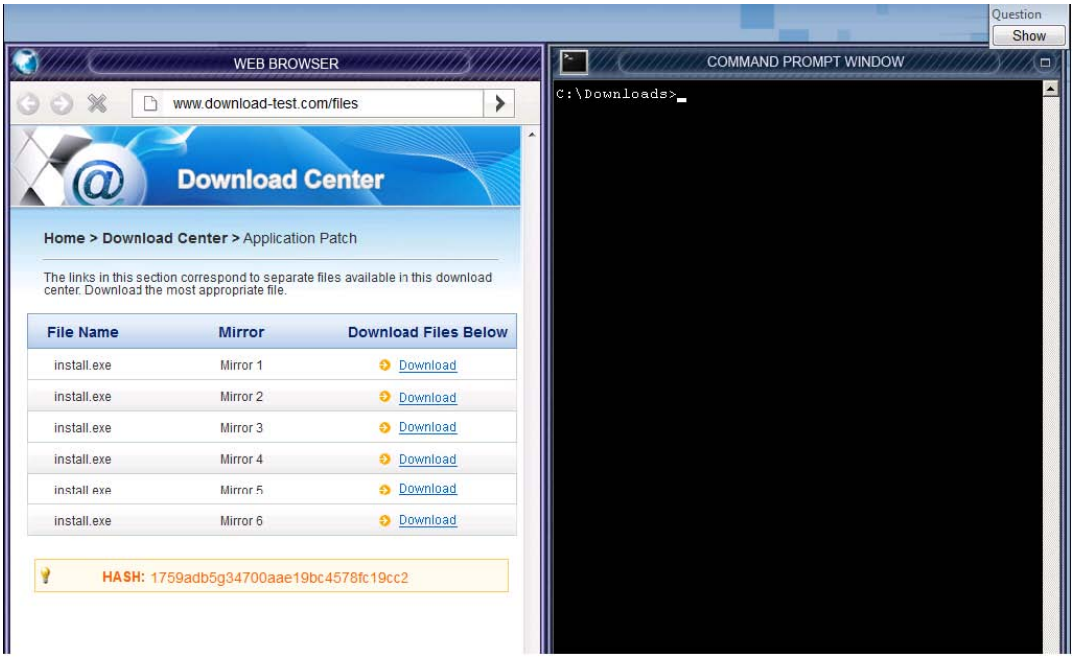
NO.14 Company ABC has grown yearly through mergers and acquisitions. This has led to over 200 internal custom web applications having standalone identity stores. In order to reduce costs and improve operational efficiencies a project has been initiated to implement a centralized security infrastructure.
The requirements are as follows:
-Reduce costs -Improve efficiencies and time to market -Manageable -Accurate identity information -Standardize on authentication and authorization -Ensure a reusable model with standard integration patterns Which of the following security solution options will BEST meet the above requirements? (Select THREE).
A. Build an organization-wide fine grained access control model stored in a centralized policy data store.
B. Implement self service provisioning of identity information, coarse grained, and fine grained access control.
C. Implement a web access control agent based model with a centralized directory model providing coarse grained access control and single sign-on capabilities.
D. Implement a web access controlled reverse proxy and centralized directory model providing coarse grained access control and single sign-on capabilities.
E. Implement automated provisioning of identity information; coarse grained, and fine grained access control.
F. Move each of the applications individual fine grained access control models into a centralized directory with fine grained access control.
G. Implement a web access control forward proxy and centralized directory model, providing coarse grained access control, and single sign-on capabilities.
Answer: A,D,E

NO.15 A security administrator is investigating the compromise of a software distribution website. Forensic analysis shows that several popular files are infected with malicious code. However, comparing a hash of the infected files with the original, non-infected files which were restored from backup, shows that the hash is the same. Which of the following explains this?
A. The infected files were using obfuscation techniques to evade detection by antivirus software.
B. The infected files were specially crafted to exploit a collision in the hash function.
C. The infected files were using heuristic techniques to evade detection by antivirus software.
D. The infected files were specially crafted to exploit diffusion in the hash function.
Answer: B

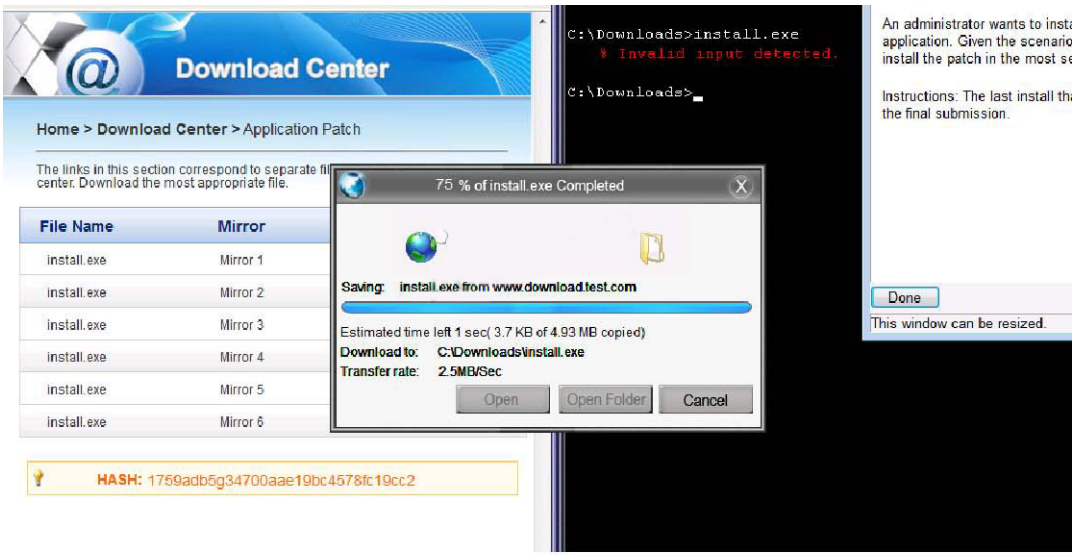
NO.16 The risk committee has endorsed the adoption of a security system development life cycle (SSDLC) designed to ensure compliance with PCI-DSS, HIPAA, and meet the organization's mission. Which of the following BEST describes the correct order of implementing a five phase SSDLC?
A. Initiation, assessment/acquisition, development/implementation, operations/maintenance and sunset.
B. Initiation, acquisition/development, implementation/assessment, operations/maintenance and sunset.

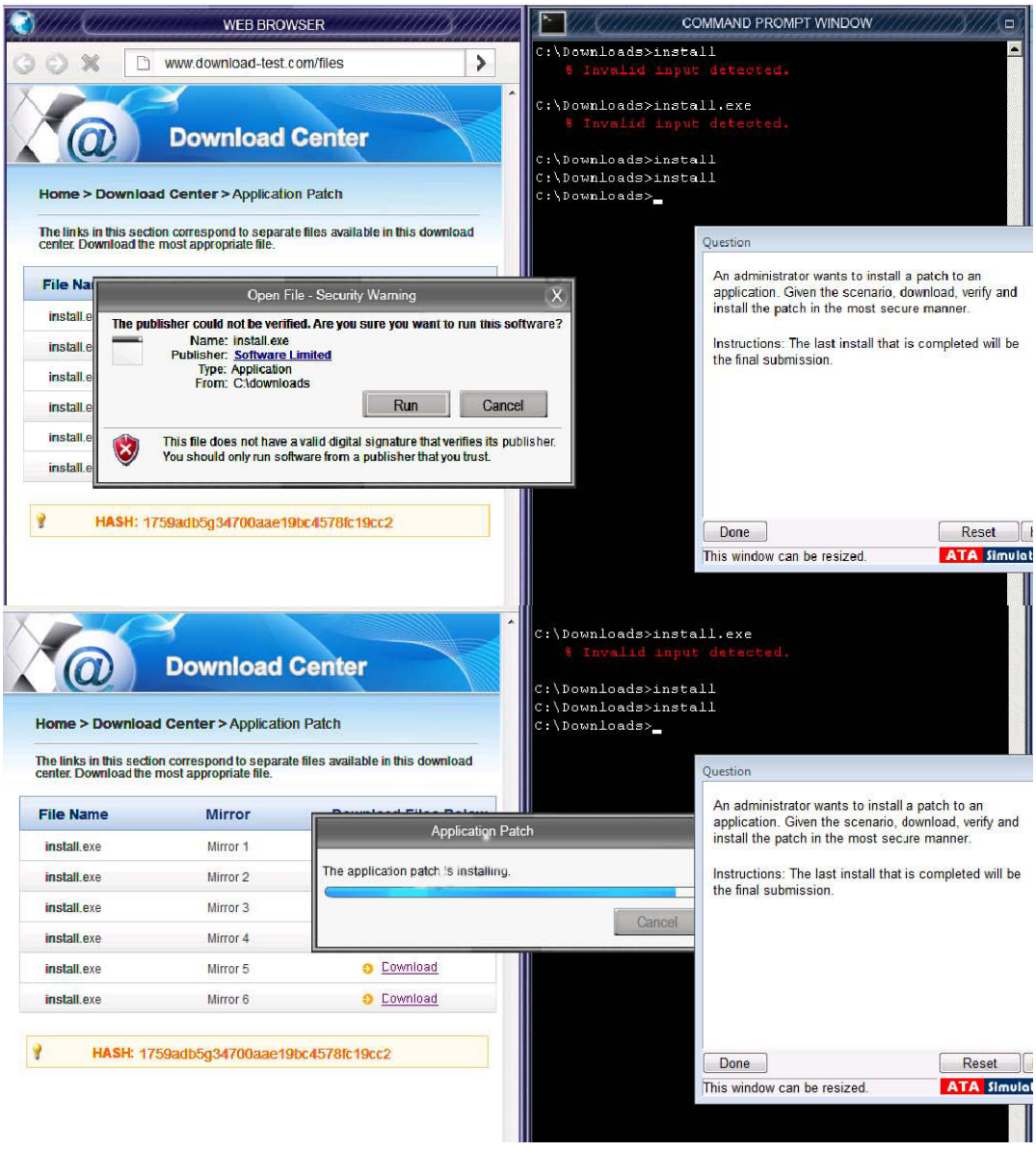
C. Assessment, initiation/development, implementation/assessment, operations/maintenance and disposal.
D. Acquisition, initiation/development, implementation/assessment, operations/maintenance and disposal.
Answer: B

NO.17 CORRECT TEXT
An administrator wants to install a patch to an application. Given the scenario, download, verify and install the patch in the most secure manner. Instructions The last install that is completed will be the final submission



Answer:
You need to check the hash value of download software with md5 utility.
Explanation:
Check the below images for more details:





NO.18 A system administrator is troubleshooting a possible denial of service on a sensitive system.

The system seems to run properly for a few hours after it is restarted, but then it suddenly stops processing transactions. The system administrator suspects an internal DoS caused by a disgruntled developer who is currently seeking a new job while still working for the company. After looking into various system logs, the system administrator looks at the following output from the main system service responsible for processing incoming transactions.

DATE/TIMEPIDCOMMAND%CPUMEM
03102014103000 2055com.proc10.2920K
03102014110000 2055com.proc12.35.2M
03102014123000 2055com.proc22.022M
03102014130000 2055com.proc33.01.6G
03102014133000 2055com.proc30.28.0G

Which of the following is the MOST likely cause for the DoS?

A. The system does not implement proper garbage collection.
B. The system is susceptible to integer overflow.
C. The system does not implement input validation.
D. The system does not protect against buffer overflows properly.

Answer: A