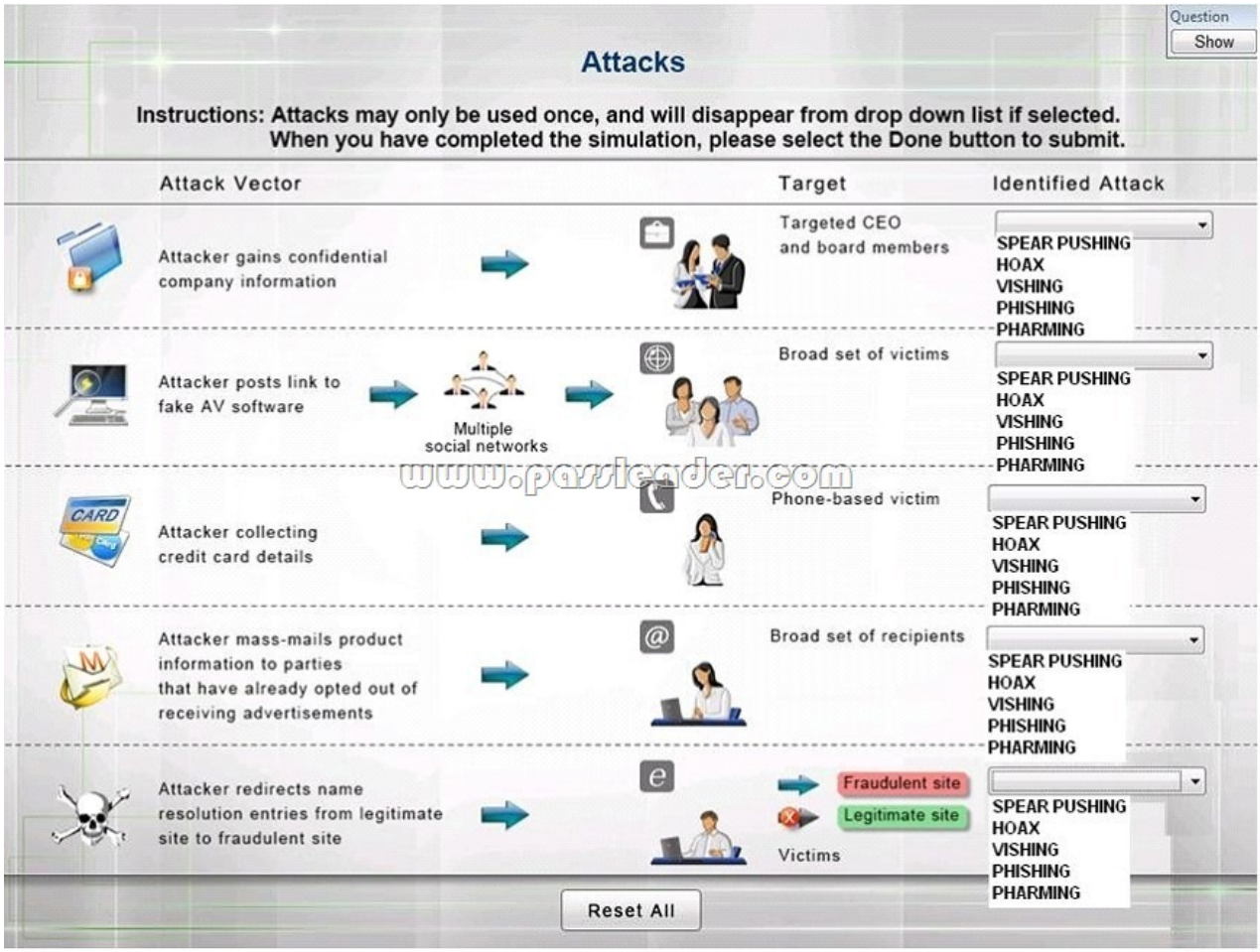
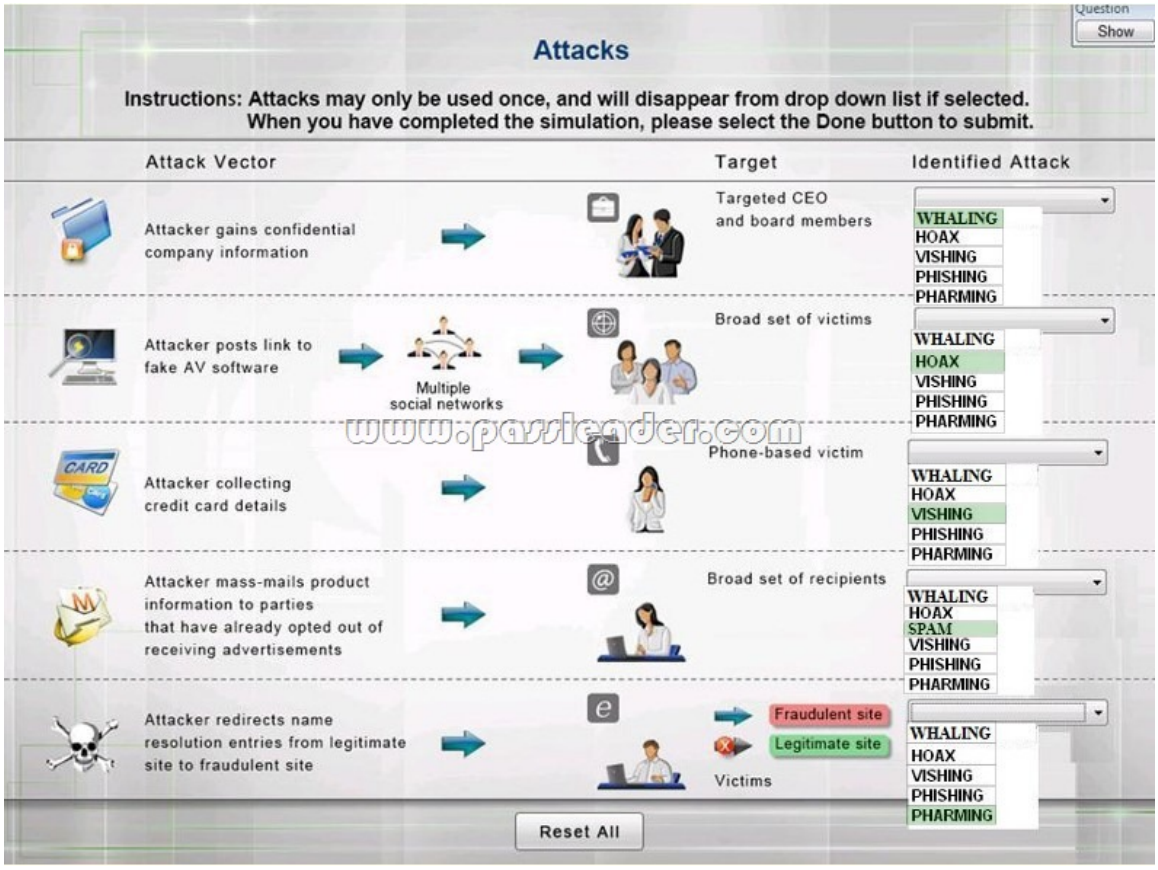
[2018 Version PassLeader Actual 182q SY0-501 PDF Exam Dumps For Free Download (Part A)

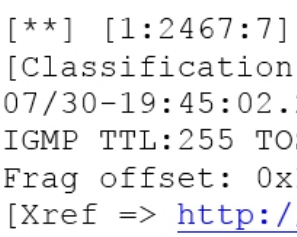
New Updated SY0-501 Exam Questions from PassLeader SY0-501 PDF dumps! Welcome to download the newest PassLeader SY0-501 VCE dumps: https://www.passleader.com/sy0-501.html (182 Q&As) Keywords: SY0-501 exam dumps, SY0-501 exam questions, SY0-501 VCE dumps, SY0-501 PDF dumps, SY0-501 practice tests, SY0-501 study guide, SY0-501 braindumps, CompTIA Security+ Exam P.S. New SY0-501 dumps PDF: https://drive.google.com/open?id=1Ei1CtZKTLawI_2jpkecHaVbM_kXPMZAu >> New SY0-401 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpcG9CWHp3bXlNTTg QUESTION 1A high-security defense installation recently began utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe? A. DeterrentB. PreventiveC. DetectiveD. Compensating Answer: A QUESTION 2An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT? A. Capture and document necessary information to assist in the response.B. Request the user capture and provide a screenshot or recording of the symptoms.C. Use a remote desktop client to collect and analyze the malware m real time.D. Ask the user to back up files for later recovery. Answer: C QUESTION 3Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices? A. ShibbolethB. RADIUS federationC. SAMLD. OAuthE. OpenlD connect Answer: B QUESTION 4An analyst wants to implement a more secure wifeless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS? A. PEAPB. EAPC. WPA2D. RADIUS Answer: C QUESTION 5A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure? A. LDAP servicesB. Kerberos servicesC. NTLM servicesD. CHAP services Answer: C QUESTION 6An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment DNSSEC at the organization? A. LDAPB. TPMC. TLSD. SSLE. PW Answer: C QUESTION 7Ann, an employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:- Slow performance.- Word documents, PDFs, and images no longer opening.- A pop-up.Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected? A. SpywareB. Crypto-malwareC. RootkitD. Backdoor Answer: D QUESTION 8A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures co have prevented this from occurring? A. Time-of-day restrictionsB. Permission auditing and reviewC. OffboardingD. Account expiration Answer: D QUESTION 9A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:- There is no standardization.- Employees ask for reimbursement for their devices.- Employees do not replace their devices often enough to keep them running efficiently.- The company does not have enough control over the devices.Which of the following is a deployment model that would help the company overcome these problems? A. BYODB. VDIC. COPED. CYOD Answer: D QUESTION 10A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:- All access must be correlated to a user account.- All user accounts must be assigned to a single individual.- User access to the PHI data must be recorded.- Anomalies in PHI data access must be reported.- Logs and records cannot be deleted or modified.Which of the following should the administrator implement to meet the above requirements? (Select THREE.) A. Eliminate shared accounts.B. Create a standard naming convention for accounts.C. Implement usage auditing and review.D. Enable account lockout thresholds.E. Copy logs in real time to a secured WORM drive.F. Implement time-of-day restrictions.G. Perform regular permission audits and reviews. Answer: ACG QUESTION 11Which of the following can be provided to an AAA system for the identification phase? A. UsernameB. PermissionsC. One-time tokenD. Private certificate Answer: A QUESTION 12HotspotSelect the appropriate attack from each drop down list to label the corresponding illustrated attack. Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.


Question
Show
Attacks
Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.
Attack Vector
Target
Identified Attack
Attacker gains confidential company information
Targeted CEO and board members
Attacker posts link to fake AV software
Multiple social networks
Broad set of victims
Attacker collecting credit card details
Phone-based victim
Attacker mass-mails product information to parties that have already opted out of receiving advertisements
Broad set of recipients
Attacker redirects name resolution entries from legitimate site to fraudulent site
Fraudulent site
Legitimate site
Victims
SPEAR PUSHING
HOAX
VISHING
PHISHING
PHARMING
Reset All

Answer:


Question
Show
Attacks
Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.
Attack Vector
Target
Identified Attack
Attacker gains confidential company information
Targeted CEO and board members
WHALING
HOAX
VISHING
PHISHING
PHARMING
Attacker posts link to fake AV software
Multiple social networks
Broad set of victims
Attacker collecting credit card details
Phone-based victim
Attacker mass-mails product information to parties that have already opted out of receiving advertisements
Broad set of recipients
SPAM
Attacker redirects name resolution entries from legitimate site to fraudulent site
Fraudulent site
Legitimate site
Victims
Reset All

Explanation:1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.2: The Hoax in this question is designed to make people believe that the fake AV (anti-virus) software is genuine.3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.4: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.http://searchsecurity.techtarget.com/definition/spear-phishing http://www.webopedia.com/TERM/V/vishing.htmlhttp://www.webopedia.com/TERM/P/phishing.html http://www.webopedia.com/TERM/P/pharming.html QUESTION 13Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords. Which of the following technical controls would help prevent these policy violations? (Select TWO.) A. Password expirationB. Password lengthC. Password complexityD. Password historyE. Password lockout Answer: AD QUESTION 14A security analyst is reviewing the following output from an IPS:



Given this output, which of the following can be concluded? (Select TWO.) A. The source IP of the attack is coming from 250.19 18.22.B. The source IP of the attack is coming from 250 19.18.71.C. The attacker sent a malformed IGAP packet, triggering the alert.D. The attacker sent a malformed TCP packet, triggering the alert.E. The TTL value is outside of the expected range, triggering the alert. Answer: BC QUESTION 15An organization finds that most help desk calls ate regarding account lockout due to a variety of applications running on different systems. Manager is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for this organization? A. Create multiple application accounts for each user.B. Provide secure tokens.C. Implement SSO.D. Utilize role-based access control. Answer: C QUESTION 16Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market? A. CompetitorB. HacktivistC. InsiderD. Organized crime Answer: A QUESTION 17When trying to log onto a company's new ticketing system, some employees receive the following message:Access denied: too many concurrent sessions.The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the MOST likely cause for this error message? A. Network resources have been exceeded.B. The software is out of licenses.C. The VM does not have enough processing power.D. The firewall is misconfigured. Answer: C QUESTION 18A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented if the administrator does not want to provide the wireless password or certificate to the employees? A. WPSB. 802.1xC. WPA2-PSKD. TKIP Answer: A QUESTION 19A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment? A. A perimeter firewall and IDSB. An air gapped compiler networkC. A honeypot residing in a DMZD. An ad hoc network with NATE. A bastion host Answer: B QUESTION

20Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet? A. The recipient can verify integrity of the software patch.B. The recipient can verify the authenticity of the site used to download the patch.C. The recipient can request future updates to the software using the published MD5 value.D. The recipient can successfully activate the new software patch. Answer: A QUESTION 21Drag and DropA security administrator is given the security and availability profiles for servers that are being deployed.1) Match each RAID type with the correct configuration and MINIMUM number of drives.2) Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements.Instructions:- All drive definitions can be dragged as many times as necessary.- Not all placeholders may be filled in the RAID configuration boxes.- If parity is required, please select the appropriate number of parity checkboxes.- Server profiles may be dragged only once.If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Answer:

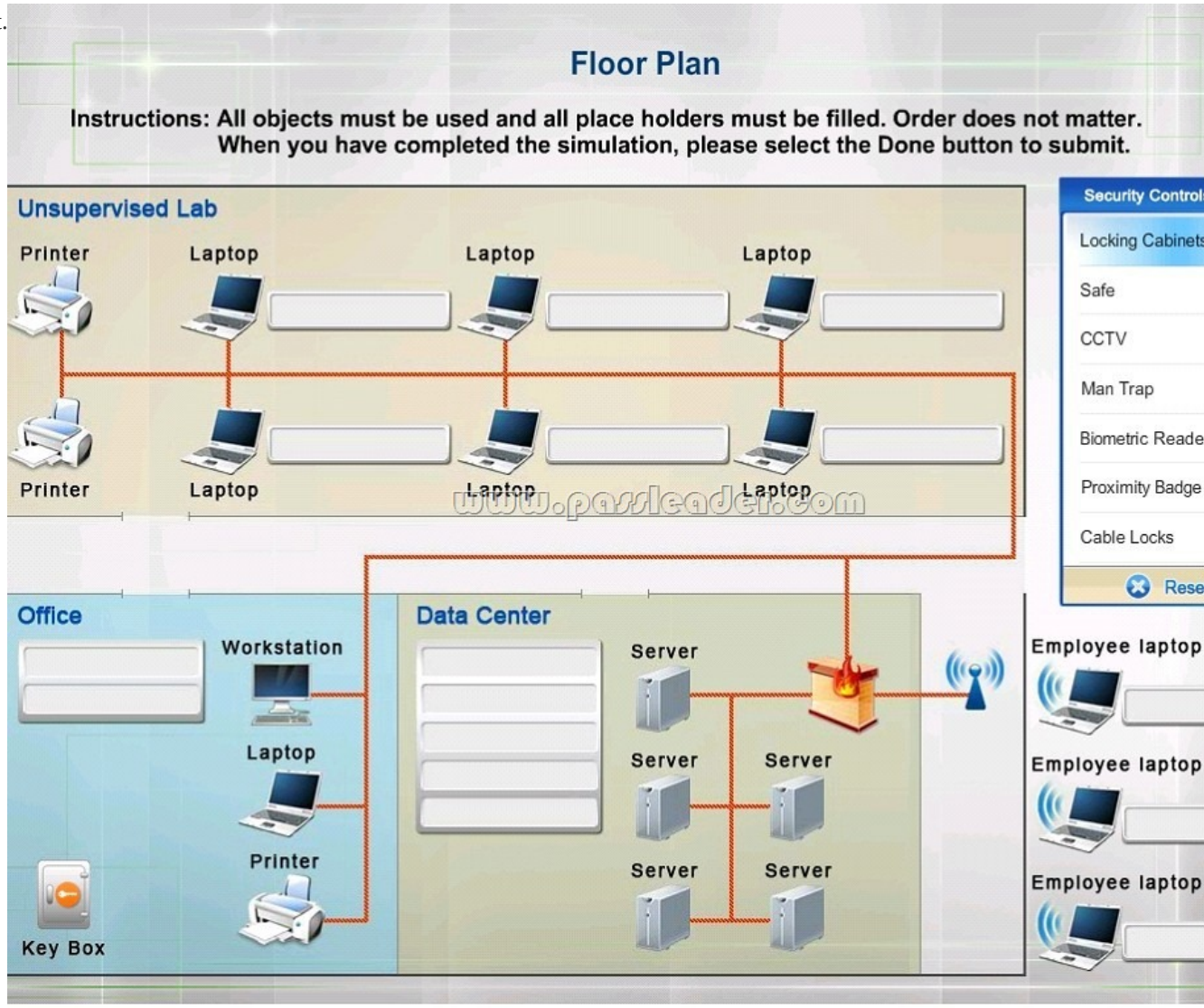


Explanation:1: RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/write operations. Striping requires a minimum of two disks and does not use parity. RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server.2: RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server. RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information. However, the parity information is distributed across all the disks. RAID-5 can recover from a sing disk failure.3: RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system.http://www.adaptec.com/en-us/solutions/raid_levels.html QUESTION 22
Refer to the following code:

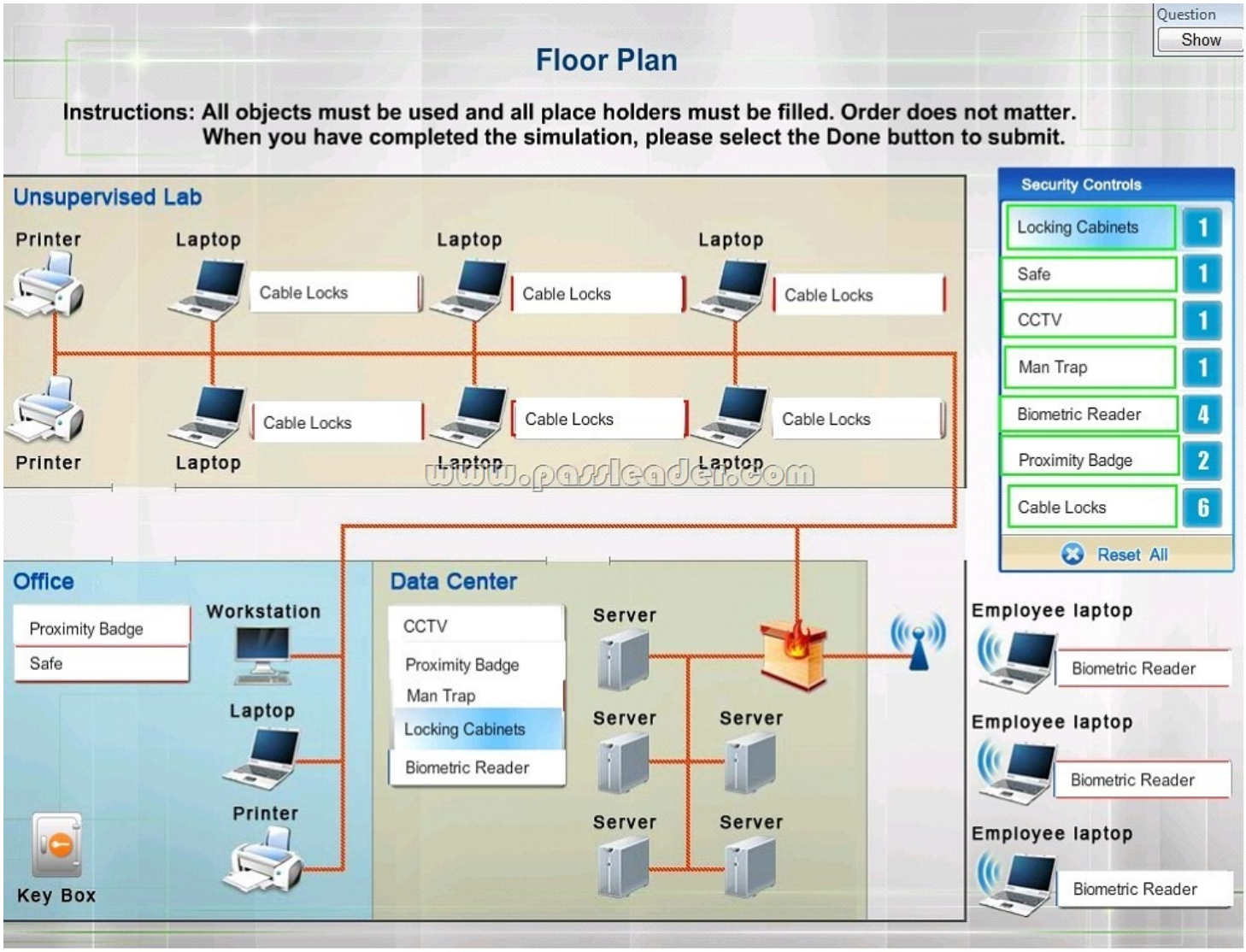
```
public class rainbow {
     public static void main (String [] args) {
          object blue = null;
          blue.hashcode (); }
}
```

Which of the following vulnerabilities would occur if this is executed? A. Page exceptionB. Pointer dereferenceC. NullPointerExceptionD. Missing null check Answer: D QUESTION 23A database backup schedule consists of weekly full backups performed on Saturday at 12:00 A.M. and daily differential backups also performed at 12:00 A.M. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery? A. 1B. 2C. 3D. 4 Answer: B QUESTION 24Which of the following technologies employ the use of SAML? (Select TWO.) A. Single sign-onB. FederationC. LDAPD. Secure tokenE. RADIUS Answer: AB QUESTION 25An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability? A. False negativeB. True negativeC. False positiveD. True positive Answer: C QUESTION 26In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has

requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested? A. ElasticityB. ScalabilityC. High availabilityD. Redundancy Answer: A QUESTION 27A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.66:66. Which of the following should the security analyst do to determine if the compromised system still has an active connection? A. tracertB. netstatC. pingD. nslookup Answer: B QUESTION 28Which of the following BEST describes an important security advantage yielded by implementing vendor diversity? A. SustainabilityB. HomogeneityC. ResiliencyD. Configurability Answer: C QUESTION 29Drag and DropYou have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.Instructions: All objects must be used and all place holders must be filled Order does not matter. When you have completed the simulation, please select the Done button to submit.



Answer:



Explanation:- Cable Locks can add a cable lock between a laptop and a desk prevents someone from picking it up and walking away.- Safe is a hardware/physical security measure.- Mantrap can be used to control access to sensitive areas.- CCTV can be used as video surveillance.- Biometric Reader can be used to control and prevent unauthorized access.- Locking Cabinets can be used to protect backup media, documentation and other physical artefacts. QUESTION 30Which of the following encryption methods does PKI typically use to securely protect keys? A. Elliptic curveB. Digital signaturesC. AsymmetricD. Obfuscation Answer: B Download the newest PassLeader SY0-501 dumps from passleader.com now! 100% Pass Guarantee! SY0-501 PDF dumps & SY0-501 VCE dumps: https://www.passleader.com/sy0-501.html (182 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New SY0-501 dumps PDF: https://drive.google.com/open?id=1Ei1CtZKTLawI_2jpkecHaVbM_kXPMZAu >> New SY0-401 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpcG9CWHp3bXlNTTg