➢ Vendor: CompTIA

➢ Exam Code: SY0-401

➢ Exam Name: CompTIA Security+ Certification Exam

➢ Question 101 – Question 200

QUESTION 101
Three of the primary security control types that can be implemented are.

A. Supervisory, subordinate, and peer.
B. Personal, procedural, and legal.
C. Operational, technical, and management.
D. Mandatory, discretionary, and permanent.

Answer: C
Explanation:
The National Institute of Standards and Technology (NIST) places controls into various types. The control types fall into three categories: Management, Operational, and Technical.

QUESTION 102
Which of the following technical controls is BEST used to define which applications a user can install and run on a company issued mobile device?

A. Authentication
B. Blacklisting
C. Whitelisting
D. Acceptable use policy

Answer: C
Explanation:
White lists are closely related to ACLs and essentially, a white list is a list of items that are allowed.

QUESTION 103
To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

A. Management
B. Administrative

C. Technical
D. Operational

Answer: C
Explanation:
controls such as preventing unauthorized access to PC's and applying screensavers that lock the PC after five minutes of inactivity is a technical control type, the same as Identification and Authentication, Access Control, Audit and Accountability as well as System and Communication Protection.

QUESTION 104
Which of the following is a management control?

A. Logon banners
B. Written security policy
C. SYN attack prevention
D. Access Control List (ACL)

Answer: B
Explanation:
Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment; and written security policy falls in this category.

QUESTION 105
Which of the following can result in significant administrative overhead from incorrect reporting?

A. Job rotation
B. Acceptable usage policies
C. False positives
D. Mandatory vacations

Answer: C
Explanation:
False positives are essentially events that are mistakenly flagged and are not really events to be concerned about. This causes a significant administrative overhead because the reporting is what results in the false positives.

QUESTION 106
A vulnerability scan is reporting that patches are missing on a server.
After a review, it is determined that the application requiring the patch does not exist on the operating system.
Which of the following describes this cause?

A. Application hardening
B. False positive
C. Baseline code review
D. False negative

Answer: B
Explanation:
False positives are essentially events that are mistakenly flagged and are not really events to be

concerned about.

QUESTION 107
Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results?

A. True negatives
B. True positives
C. False positives
D. False negatives

Answer: C
Explanation:
False positives are essentially events that are mistakenly flagged and are not really events to be concerned about.

QUESTION 108
Which of the following is an example of a false negative?

A. The IDS does not identify a buffer overflow.
B. Anti-virus identifies a benign application as malware.
C. Anti-virus protection interferes with the normal operation of an application.
D. A user account is locked out after the user mistypes the password too many times.

Answer: A
Explanation:
With a false negative, you are not alerted to a situation when you should be alerted.

QUESTION 109
A company storing data on a secure server wants to ensure it is legally able to dismiss and prosecute staff who intentionally access the server via Telnet and illegally tamper with customer data. Which of the following administrative controls should be implemented to BEST achieve this?

A. Command shell restrictions
B. Restricted interface
C. Warning banners
D. Session output pipe to /dev/null

Answer: C
Explanation:
Within Microsoft Windows, you have the ability to put signs (in the form of onscreen pop-up banners) that appear before the login telling similar information--authorized access only, violators will be prosecuted, and so forth. Such banners convey warnings or regulatory information to the user that they must "accept" in order to use the machine or network.
You need to make staff aware that they may legally be prosecuted and a message is best given via a banner so that all staff using workstation will get notification.

QUESTION 110
Joe, a security analyst, asks each employee of an organization to sign a statement saying that they understand how their activities may be monitored. Which of the following BEST describes this statement? (Select TWO).

A. Acceptable use policy
B. Risk acceptance policy
C. Privacy policy
D. Email policy
E. Security policy

Answer: AC
Explanation:
Privacy policies define what controls are required to implement and maintain the sanctity of data privacy in the work environment. Privacy policy is a legal document that outlines how data collected is secured. It should encompass information regarding the information the company collects, privacy choices you have based on your account, potential information sharing of your data with other parties, security measures in place, and enforcement. Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

QUESTION 111
Joe, a newly hired employee, has a corporate workstation that has been compromised due to several visits to P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of such web sites. Which of the following is the BEST method to deter employees from the improper use of the company's information systems?

A. Acceptable Use Policy
B. Privacy Policy
C. Security Policy
D. Human Resource Policy

Answer: A
Explanation:
Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

QUESTION 112
Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.
B. Tell the application development manager to code the application to adhere to the company's password policy.
C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.
D. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

Answer: B
Explanation:
Since the application is violating the security policy it should be coded differently to comply with the password policy.

QUESTION 113
A major security risk with co-mingling of hosts with different security requirements is:

A. Security policy violations.
B. Zombie attacks.
C. Password compromises.
D. Privilege creep.

Answer: A
Explanation:
The entire network is only as strong as the weakest host. Thus with the co-mingling of hosts with different security requirements would be risking security policy violations.

QUESTION 114
Which of the following provides the BEST explanation regarding why an organization needs to implement IT security policies?

A. To ensure that false positives are identified
B. To ensure that staff conform to the policy
C. To reduce the organizational risk
D. To require acceptable usage of IT systems

Answer: C
Explanation:
Once risks has been identified and assessed then there are five possible actions that should be taken. These are: Risk avoidance, Risk transference, Risk mitigation, Risk deterrence and Risk acceptance. Anytime you engage in steps to reduce risk, you are busy with risk mitigation and implementing IT security policy is a risk mitigation strategy.

QUESTION 115
Which of the allow Pete, a security analyst, to trigger a security alert reduce the risk of employees working in collusion to embezzle funds from their company?

A. Privacy Policy
B. Least Privilege
C. Acceptable Use
D. Mandatory Vacations

Answer: D
Explanation:
A mandatory vacation policy requires all users to take time away from work to refresh. But not only does mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels as well as an opportunity to discover fraud.

QUESTION 116
Two members of the finance department have access to sensitive information. The company is concerned they may work together to steal information. Which of the following controls could be implemented to discover if they are working together?

A. Least privilege access
B. Separation of duties
C. Mandatory access control
D. Mandatory vacations

Answer: D
Explanation:
A mandatory vacation policy requires all users to take time away from work to refresh. Mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels. Mandatory vacations also provide an opportunity to discover fraud. In this case mandatory vacations can prevent the two members from colluding to steal the information that they have access to.

QUESTION 117
One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following?

A. Mandatory access
B. Rule-based access control
C. Least privilege
D. Job rotation

Answer: C
Explanation:
A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more.

QUESTION 118
A security administrator notices that a specific network administrator is making unauthorized changes to the firewall every Saturday morning. Which of the following would be used to mitigate this issue so that only security administrators can make changes to the firewall?

A. Mandatory vacations
B. Job rotation
C. Least privilege
D. Time of day restrictions

Answer: C
Explanation:
A least privilege policy is to give users only the permissions that they need to do their work and no more. That is only allowing security administrators to be able to make changes to the firewall by practicing the least privilege principle.

QUESTION 119
Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles?

A. User rights reviews
B. Incident management
C. Risk based controls
D. Annual loss expectancy

Answer: A

Explanation:
A least privilege policy should be used when assigning permissions. Give users only the permissions and rights that they need to do their work and no more.

QUESTION 120
An IT security manager is asked to provide the total risk to the business. Which of the following calculations would he security manager choose to determine total risk?

A. (Threats X vulnerability X asset value) x controls gap
B. (Threats X vulnerability X profit) x asset value
C. Threats X vulnerability X control gap
D. Threats X vulnerability X asset value

Answer: D
Explanation:
Threats X vulnerability X asset value is equal to asset value (AV) times exposure factor (EF).
This is used to calculate a risk.

QUESTION 121
A company is preparing to decommission an offline, non-networked root certificate server. Before sending the server's drives to be destroyed by a contracted company, the Chief Security Officer (CSO) wants to be certain that the data will not be accessed. Which of the following, if implemented, would BEST reassure the CSO? (Select TWO).

A. Disk hashing procedures
B. Full disk encryption
C. Data retention policies
D. Disk wiping procedures
E. Removable media encryption

Answer: BD
Explanation:
B: Full disk encryption is when the entire volume is encrypted; the data is not accessible to someone who might boot another operating system in an attempt to bypass the computer's security. Full disk encryption is sometimes referred to as hard drive encryption.
D: Disk wiping is the process of overwriting data on the repeatedly, or using a magnet to alter the magnetic structure of the disks. This renders the data unreadable.

QUESTION 122
Identifying residual risk is MOST important to which of the following concepts?

A. Risk deterrence
B. Risk acceptance
C. Risk mitigation
D. Risk avoidance

Answer: B
Explanation:
Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition. To truly qualify as acceptance, it cannot be a risk where the administrator or manager is unaware of its existence; it has to be an identified risk for which those involved understand the potential cost or damage and agree to accept it. Residual risk is always present and will remain a risk thus it should

be accepted (risk acceptance)

QUESTION 123

A software company has completed a security assessment. The assessment states that the company should implement fencing and lighting around the property. Additionally, the assessment states that production releases of their software should be digitally signed. Given the recommendations, the company was deficient in which of the following core security areas? (Select TWO).

A. Fault tolerance
B. Encryption
C. Availability
D. Integrity
E. Safety
F. Confidentiality

Answer: DE

Explanation:

Aspects such as fencing, proper lighting, locks, CCTV, Escape plans Drills, escape routes and testing controls form part of safety controls.

Integrity refers to aspects such as hashing, digital signatures, certificates and non-repudiation - all of which has to do with data integrity.

QUESTION 124

Which of the following defines a business goal for system restoration and acceptable data loss?

A. MTTR
B. MTBF
C. RPO
D. Warm site

Answer: C

Explanation:

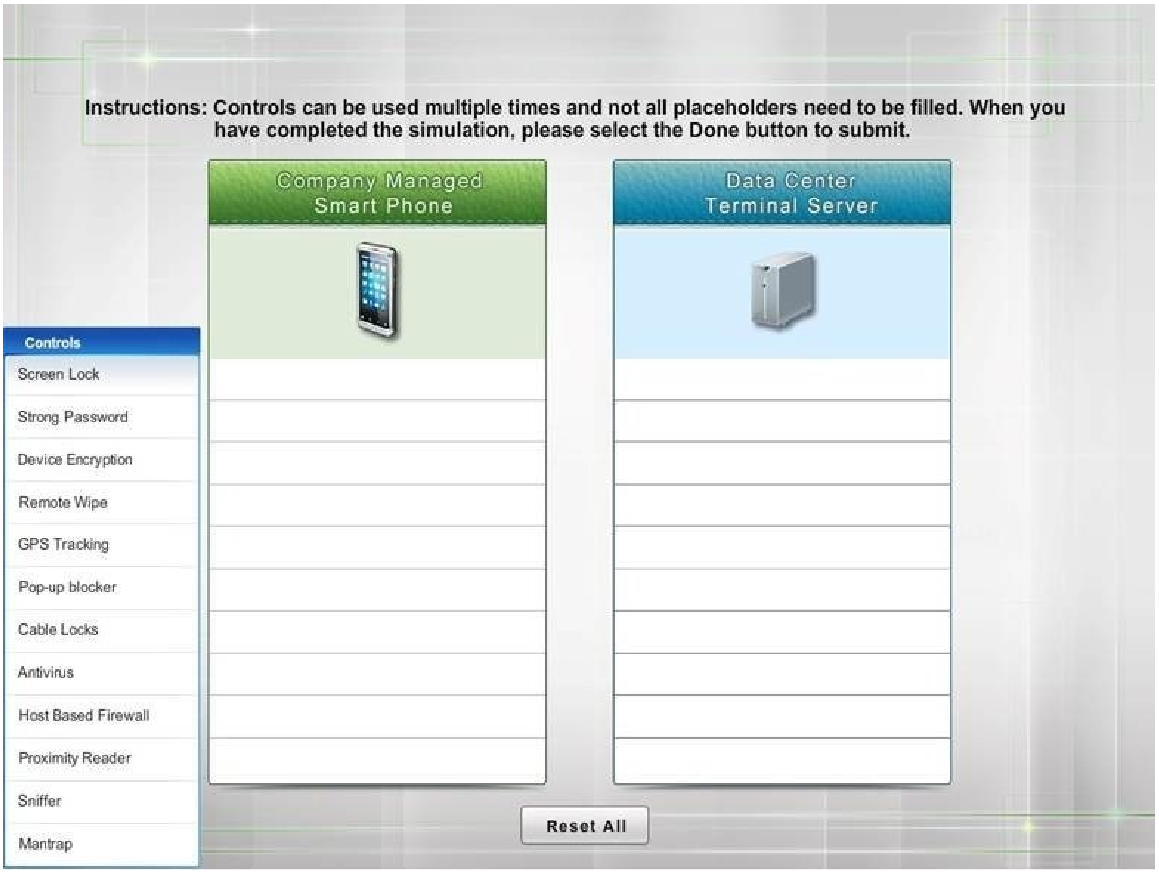
The recovery point objective (RPO) defines the point at which the system needs to be restored. This could be where the system was two days before it crashed (whip out the old backup tapes) or five minutes before it crashed (requiring complete redundancy). This is an essential business goal insofar as system restoration and acceptable data loss is concerned.

QUESTION 125

Drag and Drop Question

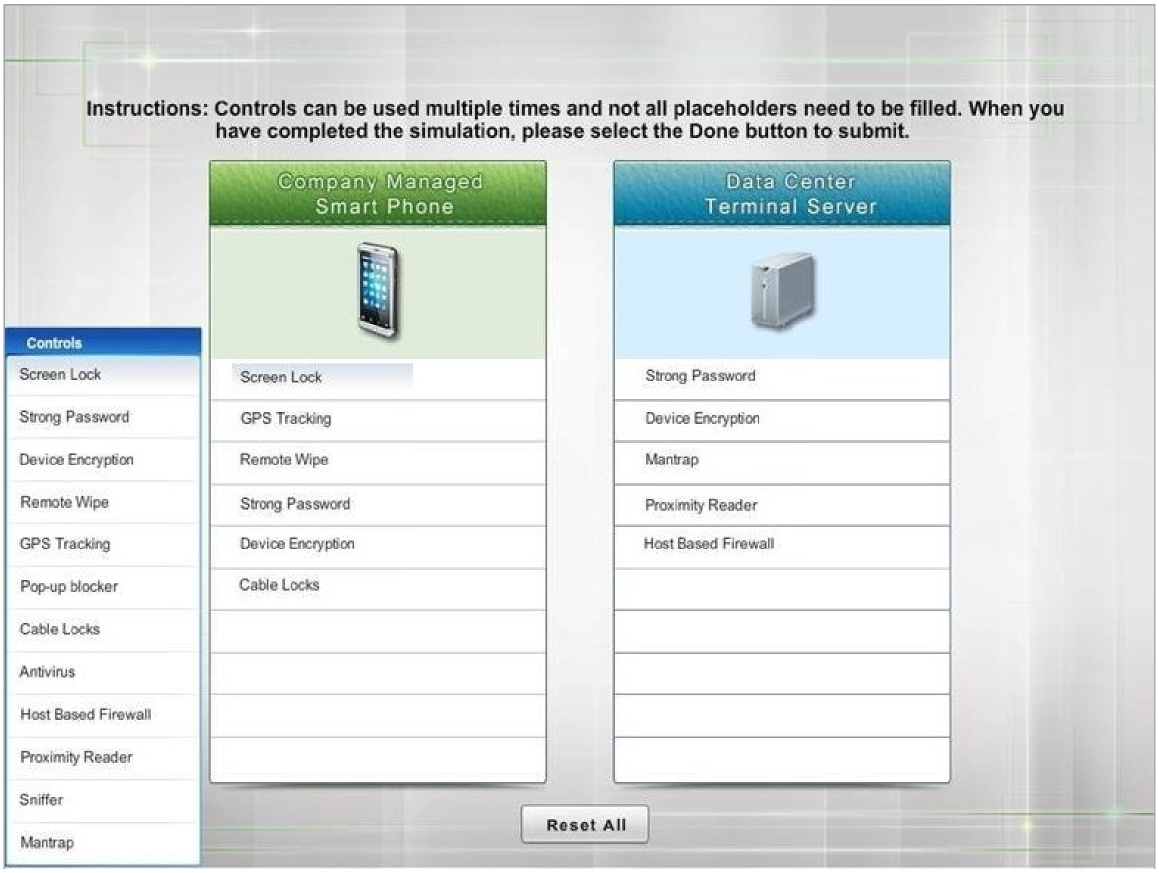
A Security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and Drop the applicable controls to each asset type.

Instructions: Controls can be used multiple times and not all placeholders needs to be filled. When you have completed the simulation, Please select Done to submit.



Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.

Answer:



Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.

Controls	Company Managed Smart Phone	Data Center Terminal Server
Screen Lock	Screen Lock	Strong Password
Strong Password	GPS Tracking	Device Encryption
Device Encryption	Remote Wipe	Mantrap
Remote Wipe	Strong Password	Proximity Reader
GPS Tracking	Device Encryption	Host Based Firewall
Pop-up blocker	Cable Locks	
Cable Locks		
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mantrap		

Explanation:
http://www.mentor-app.com/

QUESTION 126
Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years. Which of the following should Sara do to address the risk?

A. Accept the risk saving $10,000.
B. Ignore the risk saving $5,000.
C. Mitigate the risk saving $10,000.
D. Transfer the risk saving $5,000.

Answer: D
Explanation:
Risk transference involves sharing some of the risk burden with someone else, such as an insurance company. The cost of the security breach over a period of 5 years would amount to $30,000 and it is better to save $5,000.

QUESTION 127
Which of the following concepts are included on the three sides of the "security triangle"? (Select THREE).

A. Confidentiality
B. Availability

C. Integrity
D. Authorization
E. Authentication
F. Continuity

Answer: ABC
Explanation:
Confidentiality, integrity, and availability are the three most important concepts in security. Thus they form the security triangle.

QUESTION 128
Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns?

A. Hardware integrity
B. Data confidentiality
C. Availability of servers
D. Integrity of data

Answer: B
Explanation:
Data that is not kept separate or segregated will impact on that data's confidentiality maybe being compromised. Be aware of the fact that your data is only as safe as the data with which it is integrated. For example, assume that your client database is hosted on a server that another company is also using to test an application that they are creating. If their application obtains root-level access at some point (such as to change passwords) and crashes at that point, then the user running the application could be left with root permissions and conceivably be to access data on the server for which they are not authorized, such as your client database.
Data segregation is crucial; keep your data on secure servers.

QUESTION 129
Acme Corp has selectively outsourced proprietary business processes to ABC Services. Due to some technical issues, ABC services wants to send some of Acme Corp's debug data to a third party vendor for problem resolution. Which of the following MUST be considered prior to sending data to a third party?

A. The data should be encrypted prior to transport
B. This would not constitute unauthorized data sharing
C. This may violate data ownership and non-disclosure agreements
D. Acme Corp should send the data to ABC Services' vendor instead

Answer: C
Explanation:
With sending your data to a third party is already a risk since the third party may have a different policy than yours. Data ownership and non-disclosure is already a risk that you will have to accept since the data will be sent for debugging /troubleshooting purposes which will result in definite disclosure of the data.

QUESTION 130
An administrator wants to minimize the amount of time needed to perform backups during the week. It is also acceptable to the administrator for restoration to take an extended time frame.
Which of the following strategies would the administrator MOST likely implement?

A. Full backups on the weekend and incremental during the week
B. Full backups on the weekend and full backups every day
C. Incremental backups on the weekend and differential backups every day
D. Differential backups on the weekend and full backups every day

Answer: A
Explanation:
A full backup is a complete, comprehensive backup of all files on a disk or server. The full backup is current only at the time it's performed. Once a full backup is made, you have a complete archive of the system at that point in time. A system shouldn't be in use while it undergoes a full backup because some files may not get backed up. Once the system goes back into operation, the backup is no longer current. A full backup can be a time-consuming process on a large system. An incremental backup is a partial backup that stores only the information that has been changed since the last full or the last incremental backup. If a full backup were performed on a Sunday night, an incremental backup done on Monday night would contain only the information that changed since Sunday night. Such a backup is typically considerably smaller than a full backup. Each incremental backup must be retained until a full backup can be performed. Incremental backups are usually the fastest backups to perform on most systems, and each incremental backup tape is relatively small.

QUESTION 131
A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed?

A. The request needs to be sent to the incident management team.
B. The request needs to be approved through the incident management process.
C. The request needs to be approved through the change management process.
D. The request needs to be sent to the change management team.

Answer: C
Explanation:
Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. Thus the actual switch configuration should first be subject to the change management approval.

QUESTION 132
Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

A. Incident management
B. Clean desk policy
C. Routine audits
D. Change management

Answer: D
Explanation:
Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. This structured approach involves policies that should be in place and technological controls that should be enforced.

QUESTION 133
Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

A. Incident management
B. Server clustering
C. Change management
D. Forensic analysis

Answer: C
Explanation:
Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. In this case `performing updates to business critical systems.

QUESTION 134
The network administrator is responsible for promoting code to applications on a DMZ web server. Which of the following processes is being followed to ensure application integrity?

A. Application hardening
B. Application firewall review
C. Application change management
D. Application patch management

Answer: C
Explanation:
Change management is the structured approach that is followed to secure a company's assets. Promoting code to application on a SMZ web server would be change management.

QUESTION 135
Which of the following MOST specifically defines the procedures to follow when scheduled system patching fails resulting in system outages?

A. Risk transference
B. Change management
C. Configuration management
D. Access control revalidation

Answer: B
Explanation:
Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. In this case `scheduled system patching'.

QUESTION 136
A security engineer is given new application extensions each month that need to be secured prior to implementation. They do not want the new extensions to invalidate or interfere with existing application security. Additionally, the engineer wants to ensure that the new requirements are approved by the appropriate personnel. Which of the following should be in place to meet these two goals? (Select TWO).

A. Patch Audit Policy
B. Change Control Policy
C. Incident Management Policy
D. Regression Testing Policy
E. Escalation Policy

F. Application Audit Policy

Answer: BD
Explanation:
A backout (regression testing) is a reversion from a change that had negative consequences.
It could be, for example, that everything was working fine until you installed a service pack on a production machine, and then services that were normally available were no longer accessible. The backout, in this instance, would revert the system to the state that it was in before the service pack was applied. Backout plans can include uninstalling service packs, hotfixes, and patches, but they can also include reversing a migration and using previous firmware. A key component to creating such a plan is identifying what events will trigger your implementing the backout.
A change control policy refers to the structured approach that is followed to secure a company's assets in the event of changes occurring.

QUESTION 137
A user has received an email from an external source which asks for details on the company's new product line set for release in one month. The user has a detailed spec sheet but it is marked "Internal Proprietary Information". Which of the following should the user do NEXT?

A. Contact their manager and request guidance on how to best move forward
B. Contact the help desk and/or incident response team to determine next steps
C. Provide the requestor with the email information since it will be released soon anyway
D. Reply back to the requestor to gain their contact information and call them

Answer: B
Explanation:
This is an incident that has to be responded to by the person who discovered it- in this case the user. An incident is any attempt to violate a security policy, a successful penetration, a compromise of a system, or any unauthorized access to information. It's important that an incident response policy establish at least the following items:
Outside agencies that should be contacted or notified in case of an incident
Resources used to deal with an incident
Procedures to gather and secure evidence
List of information that should be collected about an incident
Outside experts who can be used to address issues if needed
Policies and guidelines regarding how to handle an incident
Since the spec sheet has been marked Internal Proprietary Information the user should refer the incident to the incident response team.
Incorrect Answers:
A: The manager may or may not be part of the incident response team.
C: The information has been marked Internal Proprietary Information and providing the information to the requestor would be in violation to the company.
D: You should have the incident response team handle the situation rather than addressing the issue yourself.

QUESTION 138
Which of the following is BEST carried out immediately after a security breach is discovered?

A. Risk transference
B. Access control revalidation
C. Change management
D. Incident management

Answer: D
Explanation:
Incident management is the steps followed when security incident occurs.

QUESTION 139
A security analyst informs the Chief Executive Officer (CEO) that a security breach has just occurred. This results in the Risk Manager and Chief Information Officer (CIO) being caught unaware when the CEO asks for further information. Which of the following strategies should be implemented to ensure the Risk Manager and CIO are not caught unaware in the future?

A. Procedure and policy management
B. Chain of custody management
C. Change management
D. Incident management

Answer: D
Explanation:
incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets).
The events that could occur include security breaches.

QUESTION 140
Requiring technicians to report spyware infections is a step in which of the following?

A. Routine audits
B. Change management
C. Incident management
D. Clean desk policy

Answer: C
Explanation:
Incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets).

QUESTION 141
Which of the following is the BEST approach to perform risk mitigation of user access control rights?

A. Conduct surveys and rank the results.
B. Perform routine user permission reviews.
C. Implement periodic vulnerability scanning.
D. Disable user accounts that have not been used within the last two weeks.

Answer: B
Explanation:
Risk mitigation is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats, monitoring network traffic, adding a firewall, and so on. User permissions may be the most basic aspect of security and is best coupled with a principle of least privilege. And related to permissions is the concept of the access control list (ACL). An ACL is literally a list of who can access what resource and at what level. Thus the best risk mitigation steps insofar as access control rights are concerned, is the regular/routine review of user permissions.

QUESTION 142

An internal auditor is concerned with privilege creep that is associated with transfers inside the company. Which mitigation measure would detect and correct this?

A. User rights reviews
B. Least privilege and job rotation
C. Change management
D. Change Control

Answer: A
Explanation:
A privilege audit is used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of an organization. This means that a user rights review will reveal whether user accounts have been assigned according to their `new' job descriptions , or if there are privilege creep culprits after transfers has occurred.

QUESTION 143
A security administrator is responsible for performing periodic reviews of user permission settings due to high turnover and internal transfers at a corporation.
Which of the following BEST describes the procedure and security rationale for performing such reviews?

A. Review all user permissions and group memberships to ensure only the minimum set of permissions required to perform a job is assigned.
B. Review the permissions of all transferred users to ensure new permissions are granted so the employee can work effectively.
C. Ensure all users have adequate permissions and appropriate group memberships, so the volume of help desk calls is reduced.
D. Ensure former employee accounts have no permissions so that they cannot access any network file stores and resources.

Answer: A
Explanation:
Reviewing user permissions and group memberships form part of a privilege audit is used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation.

QUESTION 144
Various network outages have occurred recently due to unapproved changes to network and security devices. All changes were made using various system credentials.
The security analyst has been tasked to update the security policy.
Which of the following risk mitigation strategies would also need to be implemented to reduce the number of network outages due to unauthorized changes?

A. User rights and permissions review
B. Configuration management
C. Incident management
D. Implement security controls on Layer 3 devices

Answer: A
Explanation:
Reviewing user rights and permissions can be used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation and their job descriptions. Also reviewing user rights and permissions will afford the security analyst the

opportunity to put the principle of least privilege in practice as well as update the security policy

QUESTION 145
Which of the following assets is MOST likely considered for DLP?

A. Application server content
B. USB mass storage devices
C. Reverse proxy
D. Print server

Answer: B
Explanation:
Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data.
A USB presents the most likely device to be used to steal data because of its physical size.

QUESTION 146
The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud?

A. HPM technology
B. Full disk encryption
C. DLP policy
D. TPM technology

Answer: C
Explanation:
Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. The Software as a Service (SaaS) applications are remotely run over the Web and as such requires DLP monitoring.

QUESTION 147
Which of the following is a Data Loss Prevention (DLP) strategy and is MOST useful for securing data in use?

A. Email scanning
B. Content discovery
C. Database fingerprinting
D. Endpoint protection

Answer: D
Explanation:
Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. DLP systems share commonality with network intrusion prevention systems. Endpoint protection provides security and management over both physical and virtual environments.

QUESTION 148
A customer service department has a business need to send high volumes of confidential

information to customers electronically. All emails go through a DLP scanner. Which of the following is the BEST solution to meet the business needs and protect confidential information?

A. Automatically encrypt impacted outgoing emails
B. Automatically encrypt impacted incoming emails
C. Monitor impacted outgoing emails
D. Prevent impacted outgoing emails

Answer: A
Explanation:
Encryption is done to protect confidentiality and integrity of data. It also provides authentication, nonrepudiation and access control to the data. Since all emails go through a DLP scanner and it is outgoing main that requires protection then the best option is to put a system in place that will encrypt the outgoing emails automatically.

QUESTION 149
Which of the following is a best practice when a mistake is made during a forensics examination?

A. The examiner should verify the tools before, during, and after an examination.
B. The examiner should attempt to hide the mistake during cross-examination.
C. The examiner should document the mistake and workaround the problem.
D. The examiner should disclose the mistake and assess another area of the disc.

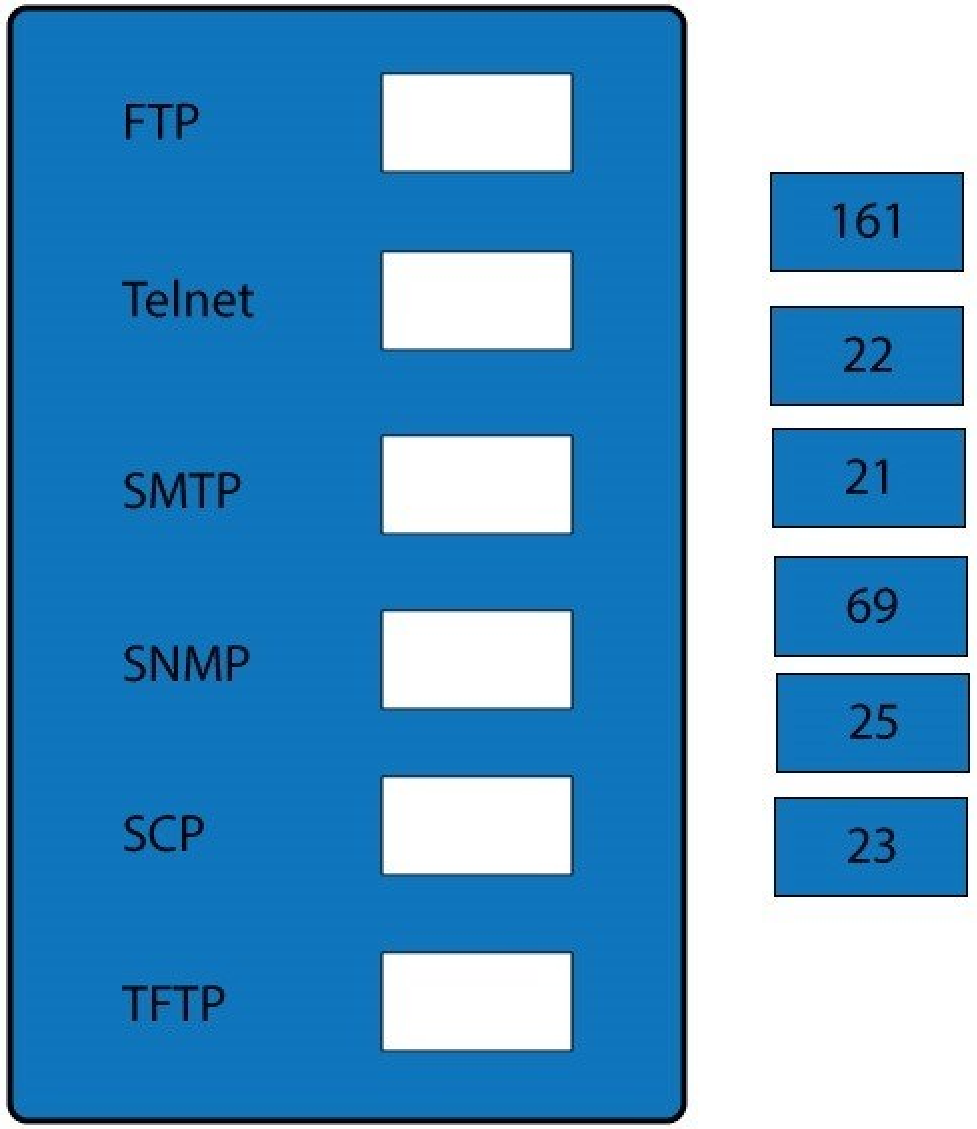
Answer: C
Explanation:
Every step in an incident response should be documented, including every action taken by end users and the incident-response team.

QUESTION 150
An incident response team member needs to perform a forensics examination but does not have the required hardware. Which of the following will allow the team member to perform the examination with minimal impact to the potential evidence?

A. Using a software file recovery disc
B. Mounting the drive in read-only mode
C. Imaging based on order of volatility
D. Hashing the image after capture

Answer: B
Explanation:
Mounting the drive in read-only mode will prevent any executable commands from being executed. This is turn will have the least impact on potential evidence using the drive in question.

QUESTION 151
Drag and Drop Questions
Drag and drop the correct protocol to its default port.



FTP

Telnet

SMTP

SNMP

SCP

TFTP

161

22

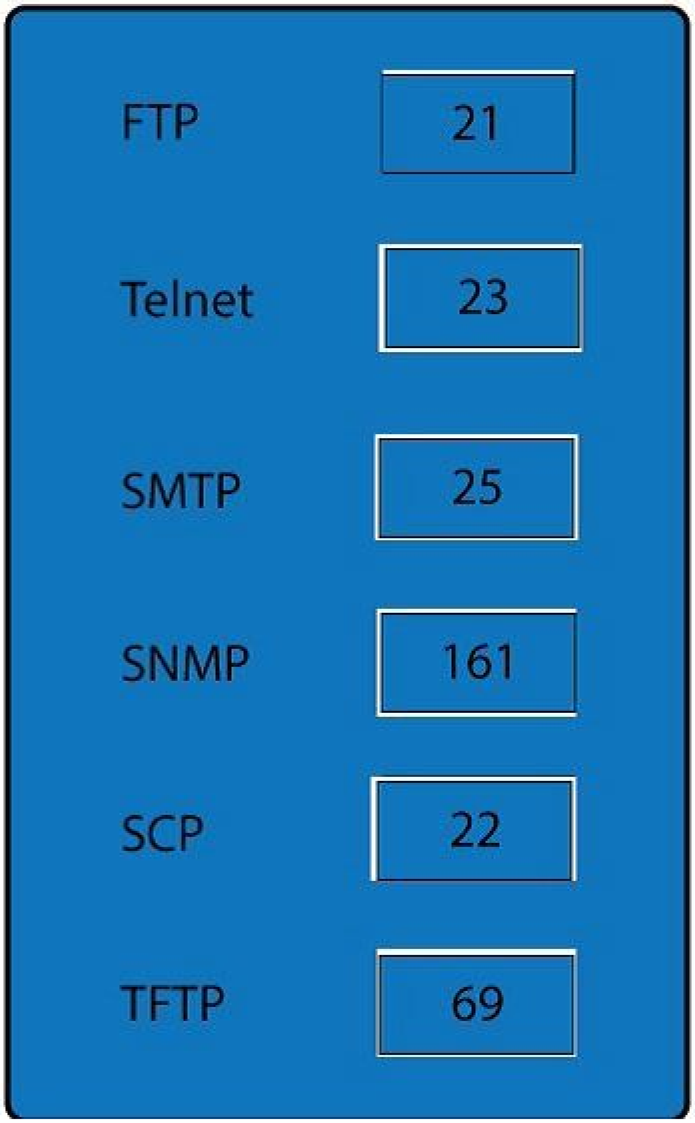
21

69

25

23

Answer:



FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

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 152

Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

A. Identify user habits
B. Disconnect system from network
C. Capture system image

D. 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 153
Computer evidence at a crime is preserved by making an exact copy of the hard disk. Which of the following does this illustrate?

A. Taking screenshots
B. System image capture
C. Chain of custody
D. 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 154
To ensure proper evidence collection, which of the following steps should be performed FIRST?

A. Take hashes from the live system
B. Review logs
C. Capture the system image
D. Copy all compromised files

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. This is essential since the collection of evidence process may result in some mishandling and changing the exploited state.

QUESTION 155
A 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=8k
B. tail -f /dev/sda > /dev/sdb bs=8k
C. dd in=/dev/sda out=/dev/sdb bs=4k
D. locate /dev/sda /dev/sdb bs=4k

Answer: C
Explanation:
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 156
A 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: B
Explanation:
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 157
A 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. Detective
B. Deterrent
C. Corrective
D. Preventive

Answer: C
Explanation:
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 158
Joe, 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: B
Explanation:
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 159

The incident response team has received the following email message.

```
From: monitor@ext-company.com
To: security@company.com
Subject: 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=john
09: 50: 22 13.10.66.5 http: //remote.site.com/logout.asp?user=anne
10: 50: 01 13.10.66.5 http: //remote.site.com/access.asp?file=movie.mov
11: 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: D

Explanation:

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 160

A 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: D

Explanation:

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 161

A 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 custody
B. Tracking man hours
C. Record time offset
D. Capture video traffic

Answer: C
Explanation:
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 162
Computer 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 capture
B. Record time offset
C. Order of volatility
D. Chain of custody

Answer: D
Explanation:
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 163
A 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 Witness
B. Data Analysis of the hard drive
C. Chain of custody
D. Expert Witness

Answer: C
Explanation:
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 164
The 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 custody
B. System image
C. Take hashes
D. Order of volatility

Answer: A
Explanation:
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 165
Which of the following is the MOST important step for preserving evidence during forensic procedures?

A. Involve law enforcement
B. Chain of custody
C. Record the time of the incident
D. Report within one hour of discovery

Answer: B
Explanation:
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 Learned
B. Preparation
C. Eradication
D. Identification

Answer: B
Explanation:
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 167
The 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 Learned
B. Eradication
C. Recovery
D. Preparation

Answer: D
Explanation:
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 168
The 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. Recovery
B. Follow-up
C. Validation
D. Identification
E. Eradication
F. Containment

Answer: D
Explanation:
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 169
Who should be contacted FIRST in the event of a security breach?

A. Forensics analysis team
B. Internal auditors
C. Incident response team
D. Software vendors

Answer: C
Explanation:
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 170
In which of the following steps of incident response does a team analyse the incident and determine steps to prevent a future occurrence?

A. Mitigation
B. Identification
C. Preparation
D. Lessons learned

Answer: D
Explanation:
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 171
After 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 management
B. Implementing policies to prevent data loss
C. User rights and permissions review
D. Lessons learned

Answer: D
Explanation:
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 172
A 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: A
Explanation:
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 173

In 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 hashes
B. Begin the chain of custody paperwork
C. Take screen shots
D. Capture the system image
E. Decompile suspicious files

Answer: AD

Explanation:

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 174

Which of the following is the LEAST volatile when performing incident response procedures?

A. Registers
B. RAID cache
C. RAM
D. Hard drive

Answer: D

Explanation:

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 175

The 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 Analysis
B. First Responder
C. Damage and Loss Control
D. Contingency Planning

Answer: B

Explanation:

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.

QUESTION 176
After a number of highly publicized and embarrassing customer data leaks as a result of social engineering attacks by phone, the Chief Information Officer (CIO) has decided user training will reduce the risk of another data leak. Which of the following would be MOST effective in reducing data leaks in this situation?

A. Information Security Awareness
B. Social Media and BYOD
C. Data Handling and Disposal
D. Acceptable Use of IT Systems

Answer: A
Explanation:
Education and training with regard to Information Security Awareness will reduce the risk of data leaks and as such forms an integral part of Security Awareness. By employing social engineering data can be leaked by employees and only when company users are made aware of the methods of social engineering via Information Security Awareness Training, you can reduce the risk of data leaks.

QUESTION 177
Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?

A. Acceptable Use Policy
B. Physical security controls
C. Technical controls
D. Security awareness training

Answer: D
Explanation:
Security awareness and training include explaining policies, procedures, and current threats to both users and management. A security awareness and training program can do much to assist in your efforts to improve and maintain security. A good security awareness training program for the entire organization should cover the following areas: Importance of security; Responsibilities of people in the organization; Policies and procedures; Usage policies; Account and password- selection criteria as well as Social engineering prevention.

QUESTION 178
Human Resources (HR) would like executives to undergo only two specific security training programs a year. Which of the following provides the BEST level of security training for the executives? (Select TWO).

A. Acceptable use of social media
B. Data handling and disposal
C. Zero day exploits and viruses
D. Phishing threats and attacks
E. Clean desk and BYOD
F. Information security awareness

Answer: DF

Explanation:

Managers/ i.e. executives in the company are concerned with more global issues in the organization, including enforcing security policies and procedures. Managers should receive additional training or exposure that explains the issues, threats, and methods of dealing with threats. Management will also be concerned about productivity impacts and enforcement and how the various departments are affected by security policies. Phishing is a form of social engineering in which you ask someone for a piece of information that you are missing by making it look as if it is a legitimate request. An email might look as if it is from a bank and contain some basic information, such as the user's name. Executives an easily fall prey to phishing if they are not trained to lookout for these attacks.

QUESTION 179

The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is:

A. Security awareness training.
B. BYOD security training.
C. Role-based security training.
D. Legal compliance training.

Answer: A

Explanation:

Security awareness and training are critical to the success of a security effort. They include explaining policies, procedures, and current threats to both users and management.

QUESTION 180

Sara, an employee, tethers her smartphone to her work PC to bypass the corporate web security gateway while connected to the LAN. While Sara is out at lunch her PC is compromised via the tethered connection and corporate data is stolen. Which of the following would BEST prevent this from occurring again?

A. Disable the wireless access and implement strict router ACLs.
B. Reduce restrictions on the corporate web security gateway.
C. Security policy and threat awareness training.
D. Perform user rights and permissions reviews.

Answer: C

Explanation:

BYOD (In this case Sara's smart phone) involves the possibility of a personal device that is infected with malware introducing that malware to the network and security awareness training will address the issue of the company's security policy with regard to BYOD.

QUESTION 181

Which of the following is the BEST reason to provide user awareness and training programs for organizational staff?

A. To ensure proper use of social media
B. To reduce organizational IT risk
C. To detail business impact analyses
D. To train staff on zero-days

Answer: B
Explanation:
Ideally, a security awareness training program for the entire organization should cover the following areas:
Importance of security
Responsibilities of people in the organization
Policies and procedures
Usage policies
Account and password-selection criteria
Social engineering prevention
You can accomplish this training either by using internal staff or by hiring outside trainers.
This type of training will significantly reduce the organizational IT risk.

QUESTION 182
Ann would like to forward some Personal Identifiable Information to her HR department by email, but she is worried about the confidentiality of the information. Which of the following will accomplish this task securely?

A. Digital Signatures
B. Hashing
C. Secret Key
D. Encryption

Answer: D
Explanation:
Encryption is used to prevent unauthorized users from accessing data.
Data encryption will support the confidentiality of the email.

QUESTION 183
Ann a technician received a spear-phishing email asking her to update her personal information by clicking the link within the body of the email. Which of the following type of training would prevent Ann and other employees from becoming victims to such attacks?

A. User Awareness
B. Acceptable Use Policy
C. Personal Identifiable Information
D. Information Sharing

Answer: C
Explanation:
Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. Employees should be made aware of this type of attack by means of training.

QUESTION 184
End-user awareness training for handling sensitive personally identifiable information would include secure storage and transmission of customer:

A. Date of birth.
B. First and last name.
C. Phone number.
D. Employer name.

Answer: A
Explanation:
Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. Date of birth is personally identifiable information.

QUESTION 185
Which of the following concepts is a term that directly relates to customer privacy considerations?

A. Data handling policies
B. Personally identifiable information
C. Information classification
D. Clean desk policies

Answer: B
Explanation:
Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record.
This has a direct relation to customer privacy considerations.

QUESTION 186
Which of the following policies is implemented in order to minimize data loss or theft?

A. PII handling
B. Password policy
C. Chain of custody
D. Zero day exploits

Answer: A
Explanation:
Although the concept of PII is old, it has become much more important as information technology and the Internet have made it easier to collect PII through breaches of internet security, network security and web browser security, leading to a profitable market in collecting and reselling PII. PII can also be exploited by criminals to stalk or steal the identity of a person, or to aid in the planning of criminal acts.
Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record.
Thus a PII handling policy can be used to protect data.

QUESTION 187
Used in conjunction, which of the following are PII? (Select TWO).

A. Marital status
B. Favorite movie
C. Pet's name
D. Birthday
E. Full name

Answer: DE
Explanation:

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. A birthday together with a full name makes it personally identifiable information.

QUESTION 188
Which of the following helps to apply the proper security controls to information?

A. Data classification
B. Deduplication
C. Clean desk policy
D. Encryption

Answer: A
Explanation:
Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use. These categories make applying the appropriate policies and security controls practical.

QUESTION 189
Which of the following security awareness training is BEST suited for data owners who are concerned with protecting the confidentiality of their data?

A. Social networking use training
B. Personally owned device policy training
C. Tailgating awareness policy training
D. Information classification training

Answer: D
Explanation:
Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use. Knowing these categories and how to handle data according to its category is essential in protecting the confidentiality of the data.

QUESTION 190
An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to prevent this in the future?

A. Business continuity planning
B. Quantitative assessment
C. Data classification
D. Qualitative assessment

Answer: C
Explanation:
Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use. Knowing how to apply these categories and matching it up with the appropriate data handling will address the situation of the data `unknown sensitivity'

QUESTION 191
What is the term for the process of luring someone in (usually done by an enforcement officer or a government agent)?

A. Enticement
B. Entrapment
C. Deceit
D. Sting

Answer: A
Explanation:
Enticement is the process of luring someone into your plan or trap.

QUESTION 192
In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

A. Security control frameworks
B. Best practice
C. Access control methodologies
D. Compliance activity

Answer: B
Explanation:
Best practices are based on what is known in the industry and those methods that have consistently shown superior results over those achieved by other means.
Furthermore best practices are applied to all aspects in the work environment.

QUESTION 193
Which of the following is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead?

A. Enticement
B. Entrapment
C. Deceit
D. Sting

Answer: B
Explanation:
Entrapment is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead. Entrapment is a valid legal defense in a criminal prosecution.

QUESTION 194
Results from a vulnerability analysis indicate that all enabled virtual terminals on a router can be accessed using the same password. The company's network device security policy mandates that at least one virtual terminal have a different password than the other virtual terminals. Which of the following sets of commands would meet this requirement?

A. line vty 0 6 P@s5W0Rd password line vty 7 Qwer++!Y password
B. line console 0 password password line vty 0 4 password P@s5W0Rd
C. line vty 0 3 password Qwer++!Y line vty 4 password P@s5W0Rd
D. line vty 0 3 password Qwer++!Y line console 0 password P@s5W0Rd

Answer: C
Explanation:
The VTY lines are the Virtual Terminal lines of the router, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them.
Two numbers follow the keyword VTY because there is more than one VTY line for router access. The default number of lines is five on many Cisco routers. Here, I'm configuring one password for all terminal (VTY) lines. I can specify the actual terminal or VTY line numbers as a range. The syntax that you'll see most often, vty 0 4, covers all five terminal access lines.

QUESTION 195
Why would a technician use a password cracker?

A. To look for weak passwords on the network
B. To change a user's passwords when they leave the company
C. To enforce password complexity requirements
D. To change users passwords if they have forgotten them

Answer: A
Explanation:
A password cracker will be able to expose weak passwords on a network.

QUESTION 196
Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss?

A. Record time offset
B. Clean desk policy
C. Cloud computing
D. Routine log review

Answer: B
Explanation:
Clean Desk Policy Information on a desk--in terms of printouts, pads of note paper, sticky notes, and the like--can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk. This will mitigate the risk of data loss when applied.

QUESTION 197
The manager has a need to secure physical documents every night, since the company began enforcing the clean desk policy. The BEST solution would include: (Select TWO).

A. Fire- or water-proof safe.
B. Department door locks.
C. Proximity card.
D. 24-hour security guard.
E. Locking cabinets and drawers.

Answer: AE
Explanation:
Using a safe and locking cabinets to protect backup media, documentation, and any other physical

artifacts that could do harm if they fell into the wrong hands would form part of keeping employees desks clean as in a clean desk policy.

QUESTION 198
XYZ Corporation is about to purchase another company to expand its operations. The CEO is concerned about information leaking out, especially with the cleaning crew that comes in at night. The CEO would like to ensure no paper files are leaked. Which of the following is the BEST policy to implement?

A. Social media policy
B. Data retention policy
C. CCTV policy
D. Clean desk policy

Answer: D
Explanation:
Clean Desk Policy Information on a desk--in terms of printouts, pads of note paper, sticky notes, and the like--can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk.

QUESTION 199
Which of the following could a security administrator implement to mitigate the risk of tailgating for a large organization?

A. Train employees on correct data disposal techniques and enforce policies.
B. Only allow employees to enter or leave through one door at specified times of the day.
C. Only allow employees to go on break one at a time and post security guards 24/7 at each entrance.
D. Train employees on risks associated with social engineering attacks and enforce policies.

Answer: D
Explanation:
Tailgating is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device. Many social engineering intruders needing physical access to a site will use this method of gaining entry. Educate users to beware of this and other social engineering ploys and prevent them from happening.

QUESTION 200
Which of the following is a security concern regarding users bringing personally-owned devices that they connect to the corporate network?

A. Cross-platform compatibility issues between personal devices and server-based applications
B. Lack of controls in place to ensure that the devices have the latest system patches and signature files
C. Non-corporate devices are more difficult to locate when a user is terminated
D. Non-purchased or leased equipment may cause failure during the audits of company-owned assets

Answer: B
Explanation:
With employees who want to bring their own devices you will have to make them understand why they cannot. You do not want them plugging in a flash drive, let alone a camera, smartphone, tablet

computer, or other device, on which company files could get intermingled with personal files. Allowing this to happen can create situations where data can leave the building that shouldn't as well as introduce malware to the system. Employees should not sync unauthorized smartphones to their work systems. Some smartphones use multiple wireless spectrums and unwittingly open up the possibility for an attacker in the parking lot to gain access through the phone to the internal network. Thus if you do not have controls in place then your network is definitely at risk.