SSCP Exams A and B (Practice)

Study online at https://quizlet.com/_ifeo7c

Which of the following tools is NOT likely to be used by a hacker	Tripwire
Which of the following would be LESS likely to prevent an employee from reporting an incident?	B. The process of reporting incidents is centralized
Which of the following would NOT violate the Due Diligence concept?	Latest security patches for servers being installed as per the Patch Management process
What is the primary goal of setting up a honeypot	To know when certain types of attacks are in progress and to learn about attack techniques so the network can be fortified.
Who is responsible for providing reports to the senior management on the effectiveness of the security controls?	Information systems auditors
Which of the following are the two MOST common implementations of Intrusion Detection Systems?	Network-based and host-based
Network-based Intrusion Detection systems	A. Commonly reside on a discrete network segment and monitor the traffic on that network segment.
Which of the following are additional terms used to describe knowledge-based IDS and behavior-based IDS?	A. signature-based IDS and statistical anomaly-based IDS, respectively
Which of the following Intrusion Detection Systems (IDS) uses a database of attacks, known system vulnerabilities, monitoring current attempts to exploit those vulnerabilities, and then triggers an alarm if an attempt is found?	Knowledge-based ID system
Knowledge-based Intrusion Detection Systems (IDS) are more common than:	C. Behavior-based IDS
Which of the following types of Intrusion Detection Systems uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host?	Anomaly Detection
What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?	Assurance procedures
What IDS approach relies on a database of known attacks	Signature-based intrusion detection
Which of the following is most likely to be useful in detecting intrusions?	C. Audit trails
Which conceptual approach to intrusion detection system is the most common?	Knowledge-based intrusion detection
Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered. There are two basic IDS analysis methods that exists. Which of the basic method is more prone to false positive?	B. Anomaly Detection
In order to enable users to perform tasks and duties without having to go through extra steps it is important that the security controls and mechanisms that are in place have a degree of?	Transparency
Which of the following is required in order to provide accountability	Audit trails
Which of the following is NOT a valid reason to use external penetration service firms rather than corporate resources?	They use talented ex-hackers
Which of the following statements pertaining to ethical hacking is incorrect?	D. Ethical hackers never use tools that have the potential of affecting servers or services.
The viewing of recorded events after the fact using a closed-circuit TV camera is considered a	Detective Control
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished	A. through access control mechanisms that require identification and authentication and through the audit function
Which of the following tools is less likely to be used by a hacker?	Tripwire
Why would anomaly detection IDSs often generate a large number of false positives?	D. Because normal patterns of user and system behavior can vary wildly
What is the essential difference between a self-audit and an independent audit?	Objectivity

QUESTION 26 A periodic review of user account management should not determine:	Strength of user passwords
Due care is not related to	Profit
Which of the following is not a preventive operational control?	Conducting security awareness and technical training
Which of the following questions are least likely to help in assessing controls covering audit trails?	B. Are incidents monitored and tracked until resolved?
What setup should an administrator use for regularly testing the strength of user passwords?	C. A standalone workstation on which the password database is copied and processed by the cracking program.
If an organization were to monitor their employees' e-mail, it should not:	Monitor only a limited number of employees
Which of the following is the BEST way to detect software license violations?	D. Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.
In what way can violation clipping levels assist in violation tracking and analysis?	A. Clipping levels set a baseline for acceptable normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.
How often should a Business Continuity Plan be reviewed?	At least once a year
Which of the following best describes what would be expected at a "hot site"?	A. Computers, climate control, cables and peripherals
Who should direct short-term recovery actions immediately following a disaster?	Disaster Recovery Manager
Which one of the following represents an ALE calculation?	A. single loss expectancy x annualized rate of occurrence.
Prior to a live disaster test also called a Full Interruption test, which of the following is most important?	Conduct of a successful Parallel Test
Which of the following should be emphasized during the Business Impact Analysis (BIA) considering that the BIA focus is on business processes?	dependencies
Which of the following recovery plan test results would be most useful to management?	list of successful and unsuccessful results
Which of the following computer recovery sites is only partially equipped with processing equipment	Warm site
Which of the following computer recovery sites is the least expensive and the most difficult to test	Cold site
Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan	A. It is unlikely to be affected by the same disaster.
Contracts and agreements are often times unenforceable or hard to enforce in which of the following alternate facility recovery agreement?	reciprocal agreement
Organizations should not view disaster recovery as which of the following?	discretionary expense
Which of the following groups represents the leading source of computer crime losses?	employees
Which of the following is the best reason for the use of an automated risk analysis tool?	Information gathering would be minimized and expedited due to the amount of information already built into the tool.
A deviation from an organization-wide security policy requires which of the following	Risk acceptance
Which of the following is biggest factor that makes Computer Crimes possible	Victim carelessness
Under United States law, an investigator's notebook may be used in court in which of the following scenarios?	To refresh the investigator's memory when testing
In addition to the Legal Department, with what company function must the collection of physical evidence be coordinated if an employee is suspected?	Human resources
To be admissible in court, computer evidence must be which of the following?	relevant
The typical computer fraudsters are usually persons with which of the following characteristics	They hold a position of trust

Once evidence is seized, a law enforcement officer should emphasize which of the following?	Chain of custody
Which of the following cannot be undertaken in conjunction or while computer incident handling is ongoing?	System development activity
Devices that supply power when the commercial utility power system fails are called which of the following?	Uninterruptable power supplies (UPS)
Within the realm of IT security, which of the following combinations best defines risk?	Threat coupled with a vulnerability
Which of the following backup sites is the most effective for disaster recovery?	Hot sites
Which of the following is NOT a transaction redundancy implementation?	on-site mirroring
Which of the following steps is NOT one of the eight detailed steps of a Business Impact Assessment (BIA)	A. Notifying senior management of the start of the assessment.
Which of the following results in the most devastating business interruptions?	Loss of data
Which of the following is the most critical item from a disaster recovery point of view?	Data
Which of the following is defined as the most recent point in time to which data must be synchronized without adversely affecting the organization (financial or operational impacts)?	Recovery Point Objective
Valuable paper insurance coverage does not cover damage to which of the following?	Money and Securities
Which of the following is covered under Crime Insurance Policy Coverage?	Money and Securities
If your property Insurance has Actual Cash Valuation (ACV) clause, your damaged property will be compensated based on:	Value of the item on the date of loss
If your property Insurance has Replacement Cost Valuation (RCV) clause your damaged property will be compensated:	B. Based on new, comparable, or identical item for old regardless of condition of lost item
A momentary power outage is a:	fault
A momentary high voltage is a	spike
UESTION 70 A momentary low voltage, from 1 cycle to a few seconds, is a	sag
A prolonged high voltage is a	surge
QUESTION 72 A prolonged complete loss of electric power is a:	blackout
QUESTION 73 A prolonged power supply that is below normal voltage is a:	brownout
Because ordinary cable introduces a toxic hazard in the event of fire, special cabling is required in a separate area provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. This area is referred to as the:	Plenum area
What is the Maximum Tolerable Downtime (MTD)	D. It is maximum delay businesses can tolerate and still remain viable
Out of the steps listed below, which one is not one of the steps conducted during the Business Impact Analysis (BIA)?	Alternate site selection
Which one of the following is NOT one of the outcomes of a vulnerability assessment	C. Formal approval of BCP scope and initiation document
The scope and focus of the Business continuity plan development depends most on	Business impact analysis
QUESTION 79 Which of the following items is NOT a benefit of cold sites	Quick recovery
Qualitative loss resulting from the business interruption does NOT usually include:	Loss of revenue
When you update records in multiple locations or you make a copy of the whole database at a remote location as a way to achieve the proper level of fault-tolerance and redundancy, it is knows as?	Shadowing

Recovery Site Strategies for the technology environment depend on how much downtime an organization can tolerate before the recovery must be completed. What would you call a strategy where the alternate site is internal, standby ready, with all the technology and equipment necessary to run the applications?	Internal Hot Site
What is the most correct choice below when talking about the steps to resume normal operation at the primary site after the green light has been given by the salvage team?	C. The least critical functions should be moved back first
What would be the Annualized Rate of Occurrence (ARO) of the threat "user input error", in the case where a company employs 100 data entry clerks and every one of them makes one input error each month?	1200
How is Annualized Loss Expectancy (ALE) derived from a threat?	SLE x ARO
QUESTION 86 What does "residual risk" mean	A. The security risk that remains after controls have been implemented
Business Continuity and Disaster Recovery Planning (Primarily) addresses the:	availability of the CIA triad
What is called an event or activity that has the potential to cause harm to the information systems or networks?	Threat
A weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks is called a ?	vulnerability
What is called the probability that a threat to an information system will materialize?	Risk
Risk mitigation and risk reduction controls for providing information security are classified within three main categories, which of the following are being used?	Physical, technical and administrative
In the course of responding to and handling an incident, you work on determining the root cause of the incident. In which step are you in?	analysis and tracking
QUESTION 93 Which of the following assertions is NOT true about pattern matching and anomaly detection in intrusion detection?	C. Stateful matching scans for attack signatures by analyzing individual packets instead of traffic streams
The IP header contains a protocol field. If this field contains the value of 51, what type of data is contained within the ip datagram?	Authentication header
Which of the following is NOT a correct notation for an IPv6 address?	D. 2001:DB8::8:800::417A
Another example of Computer Incident Response Team (CIRT) activities is:	D. Management of the network logs, including collection, retention, review, and analysis of data
Which of the following backup methods makes a complete backup of every file on the server every time it is run?	full backup method
Which of the following backup methods is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets?	full backup method
Which backup method usually resets the archive bit on the files after they have been backed up?	incremental backup method
Which backup method is used if backup time is critical and tape space is at an extreme premium?	incremental backup method
Which backup method copies only files that have changed since the last full backup, but does not clear the archive bit?	Differential backup method
Which backup method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup?	differential backup method
Which of the following backup method must be made regardless of whether Differential or Incremental methods are used?	Full Backup Method

Which of the following tape formats can be used to backup data systems in addition to its original intended audio uses?	Digital Audio Tape (DAT)
QUESTION 105 Which of the following is a large hardware/software backup system that uses the RAID technology	Tape array
This type of backup management provides a continuous on-line backup by using optical or tape "jukeboxes," similar to WORMs (Write Once, Read Many):	Hierarchical Storage Management (HSM)