1. A piece of software transmits remotely across a network to a local system and executes there. What kind of software is this?

- ☐ a. A worm
- ☐ b. A backdoor program
- ☐ c. Mobile code
- ☐ d. A logic bomb

2. Which of the following answers describes a perimeter intrusion detection system (PIDS) that sends an electrical signal down a fence cable in order to detect movement?

- ☐ a. Coaxial Strain-Sensitive Cable System
- ☐ b. Time-Domain Reflectometry System
- ☐ c. Motion Path Analysis System
- ☐ d. A Microwave Sensor System

3. A leased recovery facility is equipped with power, HVAC, telephone capabilities, and some, but not all of the equipment necessary for complete recovery. What type of recovery site is this?

- ☐ a. An external hot site
- ☐ b. A mobile hot site
- ☐ c. A warm site
- ☐ d. A cold site

4. Which answer below is the MOST accurate description of what audit logs provide with respect to security?

- ☐ a. They contain valuable information on the operation of the system
- ☐ b. They alert security professionals whenever a failed login attempt occurs
- ☐ c. They provide ways to collect audit logs across multiple systems
- ☐ d. They collect information on how the Web Server E-Commerce system is holding up to recent increased activity

5. A degausser has been used to completely wipe a disk drive, but there is still data remaining on the drive. Which answer below would be the best explanation for why this happened?

- ☐ a. The degausser had inadequate magnetic erasure capabilities
- ☐ b. The degausser was used on a solid state drive
- ☐ c. There was insufficient power to run the degausser properly
- ☐ d. The flux mechanism inside the degausser failed during the wipe.

6. In this security solution, a person has to open one door, go through it, wait for the door to close and then for authentication and authorization of some sort to be performed before the next door will open. What is this solution called?

- ☐ a. A double-door security system
- ☐ b. A mantrap system
- ☐ c. A trapdoor or backdoor system
- ☐ d. A delayed door system

7. Once an incident has happened, and the analysis has provided sufficient information, the next phase is getting the system back online is _____.

- ☐ a. Recovery
- ☐ b. Lessons learned
- ☐ c. Feedback
- ☐ d. Debriefing

8. Intrusion detection systems (IDSs) that examine network traffic to determine whether it matches a known attack are called _____.

- ☐ a. Protocol-anomaly based system
- ☐ b. Signature-matching system
- ☐ c. Statistical-anomaly based system
- ☐ d. Traffic-analysis system

9. Which intrusion detection system (IDS) approach to determining network problems uses the behavioral characteristics of a system's operation or network traffic to determine whether monitored traffic represents a risk to the overall network?

- ☐ a. Statistical anomaly detection
- ☐ b. Enunciator control
- ☐ c. Signature analysis
- ☐ d. Pattern matching

10. Which of the following BEST describes a method for displaying an information item's classification, thereby also describing the ways in which that information should be handled?

- ☐ a. Information Classification Assurance
- ☐ b. The Kerberos Ticket Granting Server's (TGS's) method of creating new service tickets
- ☐ c. Labeling and Marking
- ☐ d. A Penetration Testing Team providing an organization with a set of KPIs after it has completed its penetration test.

11. Which digital technique is most typically used for hiding information inside another file?

- [ ] a. Steganography
- [ ] b. Watermarking a document that uses internal Digital Rights protection
- [ ] c. Encrypting a document with a One-time Pad (OTP)
- [ ] d. A digital artist painting a picture over another picture

12. Which of the following is MOST likely to make a facility an unattractive target for possible intruders?

- [ ] a. CCTV systems inside and outside the buildings
- [ ] b. Large, roaming guard dogs and electrified fences
- [ ] c. Techniques that can detect body heat
- [ ] d. Coaxial strain-sensitive cables woven through a fence and loud alarm systems

13. Which of the following describes combining non-sensitive data collected from separate database sources in order to access sensitive information?

- [ ] a. Aggregation
- [ ] b. The ACID test
- [ ] c. Inference
- [ ] d. Polyinstantiation

14. Which of the following perimeter intrusion detection devices are designed specifically to detect body heat?

- [ ] a. Active infrared sensors
- [ ] b. Bi-static sensors
- [ ] c. Time domain reflectometry (TDR) sensors
- [ ] d. Passive infrared sensors

15. Audit evidence for compliance should be

- [ ] a. Kept three to seven years
- [ ] b. Deleted after the audit is complete
- [ ] c. Kept according to the retention schedule
- [ ] d. Stored indefinitely

16. With which department MUST the collection of physical evidence be coordinated if an employee is suspected of wrong doing?

- [ ] a. Physical Security
- [ ] b. Human Resources
- [ ] c. Computer Security
- [ ] d. Audit

17. What is the biggest hindrance to dealing with computer crime?

- ☐ a. Computer criminals are generally smarter than computer investigators
- ☐ b. Adequate funding to stay ahead of the computer criminals
- ☐ c. Activity associated with computer crime is truly international
- ☐ d. There are so many more computer criminals than investigators that it is impossible to keep up

18. The steps involved in handling a security incident are categorized into which of the following stages?

- ☐ a. Identification of the critical business function, define recovery objectives, ensure administrative control, containment of the problem, and follow-up analysis
- ☐ b. Establishment of the processes, conducting security education, reporting the issue to management, eradication of the problem, and follow-up analysis
- ☐ c. Establishment of the processes, identification of the problem, eradication of the problem, recovering from the incident, and follow-up analysis
- ☐ d. Identification of the problem, containment of the problem, eradication of the problem, recovering from the incident, and follow-up analysis

19. What are the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information related to?

- ☐ a. Privacy
- ☐ b. Secrecy
- ☐ c. Availability
- ☐ d. Reliability

For Questions 20 - 22: S&S Corporation's support call center is flooded with calls from customers, stating that they submitted personal information on a website, in response to an email they received from S&S Corporation.

20. The action of the first responder of the Incident Response Team is to:

- ☐ a. Report the website Uniform Resource Locaton (URL) to the Anti-Phishing Working Group
- ☐ b. Email the corporation's customers informing them of the attack
- ☐ c. Set up an automated software for customers calling the support line informing them that you are aware of the incident and working to resolve it
- ☐ d. Gather more information about the potential attack

21. The primary goal of the incident response plan is to

- ☐ a. Limit the window of opportunity for the attacker
- ☐ b. Be compliant with full-disclosure requirements and inform customers
- ☐ c. Contact law enforcement and coordinate with them
- ☐ d. Train employees and customers about the dangers of social engineering

22. In order to protect the asses, I mean assets, of S&S Corporation and their customers, the security manager should

- ☐ a. Immediately inform local news media about the event and warn customers not respond to the emails.
- ☐ b. Disconnect all outside network connections for S&S corporation and disable web site applications
- ☐ c. Alert the incident response team and coordinate with them
- ☐ d. Change the IP address and DNS information for the S&S corporation to a new source address.

23. The primary goal of computer forensics is which of the following?

- ☐ a. Report malicious activity to management
- ☐ b. Obtain evidence of malicious activity
- ☐ c. Create a record of malicious activity
- ☐ d. Mitigate damages caused by malicious activity

24. Which of the following criteria should be met for off-site storage protection for media backup?

- ☐ a. The storage site should be located at least 15 miles from the main site.
- ☐ b. The storage site should always be accessible during working hours.
- ☐ c. The storage site should always be protected by an armed guard.
- ☐ d. The storage site should guard against unauthorized access.

25. Which of the following BEST describes remote journaling?

- ☐ a. Send hourly tapes containing transactions off-site
- ☐ b. Send daily tapes containing transactions off-site
- ☐ c. Real-time capture of transactions to multiple storage devices
- ☐ d. The electronic forwarding of transactions to an off-site facility

26. In addition to maintaining a record of significant events, what other step is MOST important during a recovery procedure?

- ☐ a. Report the event to the appropriate agencies and to higher management
- ☐ b. Look for patterns that might indicate wrongdoing.
- ☐ c. Resolve disputes establishing responsibility for the recovery problems
- ☐ d. Document accomplishments for future performance reviews

27. When is the disaster actually over for a company?

- ☐ a. When all people are accounted for
- ☐ b. When all operations and people are moved back into the primary site
- ☐ c. When operations are safely moved to the off-site facility
- ☐ d. When a civil official declares that all is safe

28. Which of the following would be the MOST appropriate operational recovery strategy for a business system whose Maximum Tolerable Downtime has been determined to be three hours?

- ☐ a. Hot site
- ☐ b. Cold site
- ☐ c. Warm site
- ☐ d. Multiple processing centers/mirroring technology

29. According to local policy, disaster recovery team members meet annually to discuss business recovery strategies. Each team member describes a series of actions taken by their department in the event of an emergency. Action are critiqued based on efficiency of system recovery and impact to other business units. This is BEST described as what type of testing strategy?

- ☐ a. Checklist
- ☐ b. Structured Walk-Through
- ☐ c. Simulation
- ☐ d. Parallel Test

30. Which of these could lead to the conclusion that the disaster recovery plan may not be operational within the time frame the business needs to recover?

- ☐ a. The alternate site is a warm site
- ☐ b. Critical recovery priority levels are not defined
- ☐ c. Off-site backups are located away from the alternate site
- ☐ d. The alternate site is located 70 miles away from the primary site

31. Which of these statements pertaining to disaster recovery is incorrect?

- ☐ a. A recovery team's primary task is to get the pre-defined critical business functions at the alternate site
- ☐ b. The restoration team's task is to ensure that the primary site returns to normal business conditions
- ☐ c. The disaster recover plan should include how the company will return from the alternate site to the primary site
- ☐ d. When returning to the primary site, the most critical applications should be brought back first

32. Crisis Management planning focuses management attention on the following:

- ☐ a. Pre-planning that will enable management to anticipate and react in the event of an emergency
- ☐ b. Reacting to a natural disaster such as a hurricane or earthquake
- ☐ c. Anticipating adverse financial events
- ☐ d. IT systems restart and recovery activities

33. During the development of alternative recovery strategies, all of the following activities should be performed except:

- ☐ a. Use the prioritized business process maps developed during the BIA to map time-critical supporting resources.
- ☐ b. Develop short and long term testing and maintenance strategies
- ☐ c. Prepare cost estimates for acquisitions of continuity support resources
- ☐ d. Provide executive management with recommendations on acquiring appropriate continuity resources

34. An effective continuity plan will contain all of the following types of information except for:

- ☐ a. Prioritized list of business processes or IT systems to be recovered
- ☐ b. The business impact assessment reports
- ☐ c. Recovery team structures and assignments
- ☐ d. The primary and secondary location where backup and recovery activities will take place

35. All but one of the following are advantages of automating or utilizing continuity planning software:

- ☐ a. It standardizes training approaches
- ☐ b. It provides a platform for management and audit oversight
- ☐ c. It eases long-term continuity plan maintenance
- ☐ d. It provides business partners with an enterprise wide view of the continuity planning infrastructure

36. A company has asked its security analyst to draft a document describing due diligence practices an employee should follow when traveling for company business purposes. Which of the following combinations of information security practices is MOST effective for the "road warrior"?

- ☐ a. Hard disk encryption, shredding, and awareness of the environment
- ☐ b. Laptop cable locks, thumb drives to transport the data, and paper shredding
- ☐ c. Using File Transfer Protocol to transport data back to the office, shredding CD-ROMs, and removing the hard drive from the laptop.
- ☐ d. Using paper only, cell phones, and Internet email to conduct company business

37. All visitors entering the facility should sign in and out on a visitor's log, whether a pen and paper system or a computer-based system, to maintain accountability of who is in the facility. This system is established for what other reasons?

- ☐ a. For the purpose of detection, accountability, and the necessity for response
- ☐ b. Time frame of the visit and in the case of an emergency has accountability of everyone for safety purposes
- ☐ c. Access control and surveillance
- ☐ d. For planning assessment and the requirements of proper designation

38. Which one of these would the principal practical benefit of utilizing existing physical and procedural measures in an information system's security strategy?

- ☐ a. They offer duplication of access controls
- ☐ b. They are already tried, tested, and accepted by staff
- ☐ c. They are managed by facilities staff
- ☐ d. They are written into corporate procedures

39. Architectural and engineering drawings and sketches for a new computer site are usually provided to landlords, contractors, and vendors. Which of the following would increase the risk of accidentally disclosing possible site security vulnerability on those plans?

- ☐ a. Require all companies to sign a non-disclosure agreement.
- ☐ b. Assign all documents an unclassified status and keep them in an area where they are readily accessible to those working on the project
- ☐ c. Review all engineering drawings and riser diagrams for labels such as "Computer Room" on diagrams where labels may not by necessary
- ☐ d. Use labels of "Equipment", "storage", or "future" where any room designations are needed, regardless of what is actually inside the room

40. Which of the following is the BEST way to prevent unauthorized access through an employee entrance?

- ☐ a. Policy
- ☐ b. Waist height turnstile
- ☐ c. Training
- ☐ d. Mantrap

41. A physical access control technique that requires two keys to be turned simultaneously to enter or activate a system is called _____.

- ☐ a. Dual control
- ☐ b. Double entry
- ☐ c. Mutual exclusion
- ☐ d. Two-factor

42. Which of these keys will the sender never use?

- ☐ a. Receiver's Public
- ☐ b. Receiver's Private
- ☐ c. Sender's Public
- ☐ d. Sarah's Private

43. An incident scene is _____

- ☐ a. the location where the crime was committed.
- ☐ b. the location where the evidence might be found
- ☐ c. the location described in the search warrant
- ☐ d. the location where the computer was used or stored

44. Scientific Working Group for Digital Evidence (SWGDE) principles include all of the following EXCEPT:

- ☐ a. a named individual responsible for any actions taken on the evidence while in his possession.
- ☐ b. seized digital evidence cannot be changed without making it inadmissible.
- ☐ c. all forensic and procedural best practices must be observed.
- ☐ d. the person accessing the evidence must be trained for that purpose.

45. Which of the following BEST describes the differences in software certification and accreditation activities?

- ☐ a. Accreditation occurs at the source code level, while certification occurs at the executable code level
- ☐ b. Certification means you can commence a development project, accreditation means that you can dispose of a software project
- ☐ c. Certification precedes accreditation
- ☐ d. Accreditation means you have management's okay to go into production, certification means you have chosen the software development language

Questions 46 - 49: You are the Incident Investigations Manager. The head auditor approaches you in confidence saying that the total monies in the organization's bank accounts is significantly less that that shown in the books and records of the business. You launch an investigation. Answer the following questions based upon these facts.

46. Your company has consolidated log files via a Security Information Even Management (SIEM) system. Which of these steps should be done first?

- ☐ a. Ask HR to get updated permission from all financial service employees to inspect their personal bank accounts.
- ☐ b. Ask the system administrator to freeze all financial transactions
- ☐ c. Arrange for a forensic image of the SIEM server log database
- ☐ d. Contact management for permission to begin the investigation

47. The log files are, of course, quite large. :-) You can run an inquiry to extract records of users who have logged in outside of business hours

- ☐ a. clipping
- ☐ b. filtering
- ☐ c. subset examinations
- ☐ d. the road to inadmissibility

48. Your investigation has identified a clear suspect. To confirm your beliefs, you add additional logging to cover every action that person takes. In many countries, the evidence that is collected will be _____.

- ☐ a. admissible under the silver platter doctrine
- ☐ b. admissible because your company owns the machines on which the log files reside
- ☐ c. inadmissible because you had no search warrant
- ☐ d. inadmissible because it was not captured in the ordinary course of business

49. Due to the fact that the amount of money embezzled was great , you decide to contact law enforcement, at which point they take over the case. One of the investigating officers asks you do to additional logging because they do not have the skill set to do it themselves. Would this data be admissible?

- ☐ a. This data is admissible under the plain view doctrine
- ☐ b. This data is admissible under the silver platter doctrine
- ☐ c. This data is admissible as a hearsay exception
- ☐ d. This data is admissible only if law enforcement has a valid search warrant for the data

50. Deep-packet inspection is done by a _____.

- ☐ a. DLP system
- ☐ b. Stateful firewall
- ☐ c. NIPS system
- ☐ d. HIPS system

51. Separation of duties should be implemented by _____

- ☐ a. in all areas
- ☐ b. in all areas that could be compromised by a disgruntled employee
- ☐ c. in all areas where the risk outweighs the cost
- ☐ d. in all areas where it is mandated by law or regulation

52. The data owner is NOT responsible for _____

- ☐ a. classification of data
- ☐ b. determining the need-to-know
- ☐ c. identifying data that has become obsolete
- ☐ d. understanding the replacement cost of the data

53. Which of the following is the LEAST essential component of a Service Level Agreement?

- ☐ a. Termination of the agreement procedures
- ☐ b. Description of items subject to Non-Disclosure
- ☐ c. Fines or penalties for non-compliance
- ☐ d. Arbitration clause

54. While there are several incident response frameworks, they tend to agree on three common components. Which of these is NOT one of those framework components?

- ☐ a. Creation of a response capability
- ☐ b. Activating the team
- ☐ c. Incident handling and response
- ☐ d. Recovery and feedback

55. What is the difference between an incident and an event?

- ☐ a. No difference, they are the same
- ☐ b. An event is something that can be measured, an incident is an event that can cause harm.
- ☐ c. An incident is something that can be measure, an event is an incident that can cause harm
- ☐ d. An event will trigger an investigation, an incident will trigger litigation

56. Which of these Business Continuity Planning statements is TRUE?

- ☐ a. During recovery, least critical functions are addressed first
- ☐ b. Recovery can be delayed until the arrival of the salvage and recovery team to complete its work
- ☐ c. "Recovery" is what we do on the way out, "Restoration" is what we do upon returning to the original (or new, permanent) site
- ☐ d. A vendor hot site is suitable for long term outages

57. The badge reader at the employee entrance failed, so a guard posted to examine IDs visually. This is an example of a _____

- ☐ a. corrective control
- ☐ b. physical control
- ☐ c. detective control
- ☐ d. compensating control

58. Which statement is LEAST accurate? Fire doors _____

- ☐ a. should open out.
- ☐ b. should close automatically
- ☐ c. should be solid, not hollow
- ☐ d. should be metal

59. Which of these intrusion sensors is always active?

- ☐ a. microwave sensor
- ☐ b. acoustic sensor
- ☐ c. vibration sensor
- ☐ d. infrared sensor

60. A hardened hinge is _____

- ☐ a. a steel hinge laminated with titanium
- ☐ b. a steel cap on the hinge to prevent hinge removal
- ☐ c. a dead bolt lock that has a key or lever on one side and is not visible on the other side of the door
- ☐ d. a dead bolt lock that has a key on both sides of the door

61. What feature of a fireproof safe actually makes them fireproof?

- ☐ a. they are made of metal, which does not burn
- ☐ b. they are airtight, thus no oxygen equals no fire
- ☐ c. there are fire suppression chemicals "painted" on the inside walls
- ☐ d. they are so thick the heat cannot penetrate