CyberRookie CSX Fundamentals - Mock Exam 5

Friday, September 13, 2019 3:00 PM

Section 5 - INCIDENT RESPONSE

1. An _____ is any change, error or interruption within an IT infrastructure, such as a crash, disk error or a user forgetting their password.

a) Incident

b) Event

c) None of the above

2. A _____ violation or imminent threat of violation of computer polices, acceptable use policies or standard practices.

a) Incident

b) Event

c) None of the above

3. A cybersecurity incident is an adverse event that negatively impacts the:

a) Accessibility, availability, agility

b) Moral, profit, business department

c) Confidentiality, integrity, availability

d) None of the above

4. Why do we need incident response?

a) Adequate incident response planning and implementation allows organization to respond to an incident in a systematic manner that is more effective

b) Guarantees security for the organization

c) Doesn’t do anything

d) Responds to management concerns

5. Elements of an Incident Response Plan (IRP) include:

a) Preparation, indemnity, containment, eradication, recovery, lessons learned

b) Preparation, identification, containment, eradication, restoration, lessons learned

c) Preparation, identification, consent, eradication, recovery, lessons learned

d) Preparation, identification, containment, eradication, recovery, lessons learned

6. RTO, BCP, SDO are part of what element of the Incident Response Plan (IRP):

a) Identification

b) Containment

c) Recovery

d) Lessons learned

7. This element of the Incident Response Plan (IRP) deals with the next step after the root cause of the incident has be determined:

a) Identification

b) Eradication

c) Recovery

d) Lessons learned

8. This element in the Incident Response Plan (IRP) aims to verify if an incident has happened and to find out more details about an incident:

a) Identification

b) Containment

c) Recovery

d) Lessons learned

9. When trying to preserve evidence, why is rebooting a system a bad idea?

a) Wrong, it is a good idea, it speeds things up

b) Rebooting the system or accessing files could result in evidence being lost

c) The boot up sequence can delay the investigation

d) The administrator might not be around if something goes wrong

10. For evidence to be admissible in a court of law, the chain of custody needs this information?

a) All the employees name and email addresses to contact

b) The serial numbers of all servers involved

c) The names of all IT security managers

d) Who had access to the evidence (chronological manner)

11. Label the diagram (left to right) - select the right term for the four major considerations in the chain of events in regards to evidence in digital forensics:

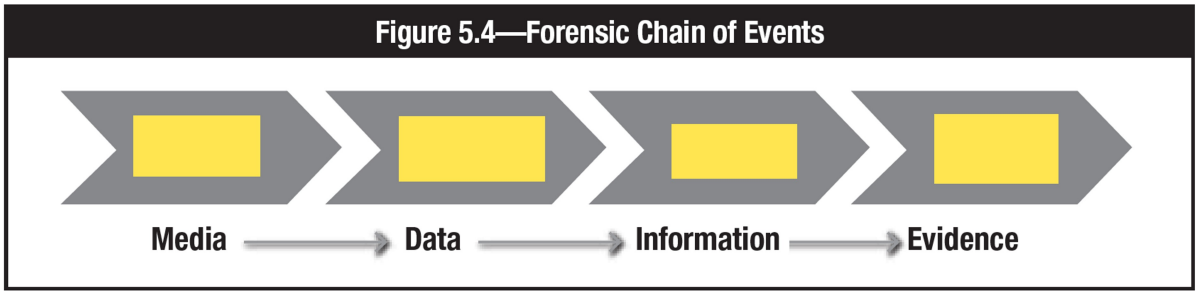
a) Preserve, Present, Identify, Analyze

b) Present, Perserve, Analyze, Identify

c) Analyze, Perserve, Present, Identify

d) Identify, Perserve, Analyze, Present

Graphic for Question 11



12. Imaging is a process in forensics, it involves:

a) Imaging involves taking an image of the servers for evidence

b) Imaging is imitating the processing server through a software image

c) Imaging process makes a copy of the serial numbers of the entire server's hardware

d) Is a process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be preformed.

13. Digital forensic tools can be sorted into four categories:

a) Computer, Memory, Mobile devices, Network

b) Computer, Servers, Software, Hardware

c) Memory, Hard drives, CDs, USB drives

d) Finger print powder, video evidence, witness statements

14. The purpose of anti-forensic tools to:

a) Harden evidence in a forensic operation

b) To make it easier to find evidence information

c) To provide a better lab environment to investigate evidence

d) Make it difficult or impossible for investigators retrieve information

15. The purpose of a Business Continuity Plan (BCP)and Disaster Recovery Plan (DRP) is to:

a) Improve profits in times of business crisis

b) Continue to operate in times of problems in the organization

c) Continue to offer critical services in the event of disruption and to survive a disastrous interruption to activities

d) Continue to offer revenue to shareholders in the event of disruption and to survive a disastrous interruption to activities

16. Arrange the steps of the incident response process into the correct order.

A. Mitigation and recovery, Investigation, Postincident analysis, Preparation, Detection and analysis

B. Investigation, Detection and analysis, Postincident analysis, Preparation, Mitigation and recovery

C. Postincident analysis, Postincident analysis, Detection and analysis, Mitigation and recovery

D. Preparation, Detection and analysis, Investigation, Mitigation and recovery, Postincident analysis

E. Detection and analysis, Postincident analysis, Preparation, Mitigation and recovery, Preparation

17. Which element of an incident response plan involves obtaining and preserving evidence?

A. Preparation

B. Identification

C. Containment

D. Eradication

18. Select three. The chain of custody contains information regarding:

A. disaster recovery objectives, resources and personnel.

B. who had access to the evidence, in chronological order.

C. labor, union and privacy regulations.

D. proof that the analysis is based on copies identical to the original evidence.

E. the procedures followed in working with the evidence.

19. NIST defines a(n) _____ as a "violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."

A. Disaster

B. Event

C. Threat

D. Incident

20. Select all that apply. A business impact analysis (BIA) should identify:

A. the circumstances under which a disaster should be declared.

B. the estimated probability of the identified threats actually occurring.

C. the efficiency and effectiveness of existing risk mitigation controls.

D. a list of potential vulnerabilities, dangers and/or threats.

E. which types of data backups (full, incremental and differential) will be used.

21. A major incident which has grown out of control and increased in severity is called a(n):

Crisis

Event

Incident

Emergency

22. What is a key difference between an incident and an event?

An incident implies a violation or imminent threat, an event does not

An event implies a violation or imminent threat, an incident does not

Events negatively impacts the confidentiality, integrity and availability, incidents do not

Incident and event means the same thing

23. Which of the following is an example of a security incident?

System crash

Disk error

User forgetting their password

Denial of service

24. An individual gains logical or physical access without permission to a network, system, application, data or other resource. This describes which incident category?

Category 1: Unauthorized access

Category 2: Denial of service

Category 4: Improper usage

Category 5: Scans/probes/improper access

25. Fallback plans may be invoked in the event of a(n):

Emergency

Disaster

Crisis

Incident

26. Technical information security incidents may involve:

Viruses, malware or denial-of-service (DoS)

System failure, social engineering or viruses

Viruses, denial-of-service or system failure

Malware, system failure or social engineering

27. The strategy used by an enterprise to respond to disruption of critical business processes is called a:

Business continuity plan (BCP)

Service delivery objective (SDO)

Computer emergency response team (CERT)

Disaster response plan (DRP)

28. Incident response includes which of the following activities?

Preparation, detection, recovery and post incident activity

Preparation, alignment and response

Preparation, detection, and post incident activity

Preparation, analysis, alignment and post incident activity

29. Obtaining and preserving evidence, documenting action and managing public communications are actions associated with:

Incident containment

Incident response

Incident eradication

Incident preparation

30. Log data overload can be mitigated by employing:

Security event management (SEM)

Security response plans

Computer security incident response teams (CSIRT)

Business continuity plans (BCP)

31. Incident preparation includes all of the following except:

Establish approach to handling incidents

Establish communication plan with stakeholders

Develop incident reporting criteria

Establish chain of custody

32. Post-incident activities typically include which of the following? Select all that apply.

Writing an incident report

Proposing improvements

Communicating findings to key stakeholders

Declaring normal operation

33. Assigning ownership and establishing chain of custody are part of which incident response plan activity?

Preparation

Identification

Containment

Eradication

34. A business impact analysis (BIA) provides the basis for which of the following? Select all that apply.

Recovery time objectives

Recovery point objectives

Maximum tolerable outages

Service delivery objectives

35. The most important objective of a business continuity plan (BCP) is:

Ensuring safety and security of human life

Maintaining operations critical to survival of the organization

Defining evacuation procedures

Outlining a step-by-step explanation of the recovery plan

36. The process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible for any reason is called:

Data recovery

Backup

Business continuity

Incident recovery

37. In order for a business continuity plan (BCP) to be effective, it must:

Be documented on paper

Be aligned with the strategy of the organization

Be tested regularly

Be approved by senior management

38. The business impact analysis (BIA) should consider which of the following critical resources? Select all that apply.

Potential vulnerabilities

Probability of occurrence of threats

Human, data and infrastructure resources

Efficiency and effectiveness of risk countermeasures

39. In a disaster recovery plan (DRP), the last known point of good data is identified as:

Recovery point objective

Recovery time objective

Full backup

Data recovery

40. The amount of time allowed for the recovery of a business function or resource after a disaster occurs is called:

Recovery point objective

Recovery time objective

Service delivery objective

Maximum tolerable outages

Back

Next