CyberRookie CSX Fundamentals - Mock Exam 2

Wednesday, October 30, 2019 3:46 PM

Section 2 - CYBERSECURITY CONCEPTS

1. Read the description and match the correct column word to describe it (6 marks):

A: Residual risk

B: Vulnerability

C: Inherent risk

D: Asset
E: Risk
F: Threat

_____The combination of the probability of an event and its consequence (ISO/IEC 73). Risk is mitigated through the use of controls or safeguards

_____Even after safeguards are in place, there will always be residual risk, defined as the remaining risk after management has implemented a risk response

_____The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)

_____Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation

_____A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

_____Anything (e.g., object, substance, human) that is capable of acting against an asset that can result in harm

2. COBIT 5 for Risk, ISO31000:2009, IEC 31010:2009, ISO/IEC 27001:2013, are examples of :
a) Rules and regulations
b) Frameworks and standards
c) Software to asses risk
d) Policy templates for organizations

3. Review the NIST diagram, select the correct workflow order:
a) Adverse impact, Vulnerability, Threat event, Threat source

b) Threat event, Adverse impact, Threat source, Vulnerability
c) Vulnerability, Threat source, Threat event, Adverse impact
d) Threat source, Threat event, Vulnerability, Adverse impact
NIST Diagram (Question 3)

4. Risk scenario structure includes the following components:
e) Actor, threat type, policies
f) Threat type, Asset/Resources, frameworks
g) Event, logs, story lines, platform
h) Actor, threat type, event, asset/resources, time

5. A _____ approach to scenario development is based on understanding business goals and how a risk event could affect the achievement of those goals.
a) Management
b) Bottom-up
c) Top-down
d) Cybersecurity

6. The measure of frequency of which an event may occur is known as:
a) Likelihood (also called probability)
b) Criticality
c) Time
d) Chance

7. Three different approaches to implementing cybersecurity, include:
a) Ad-hoc, risk-based, compliance-based
b) Penetration test, hackathon, port scanning
c) Contracts, regulations, bi-laws
d) Employee monitoring, compliance, policies

8. While risk is measured by potential activity, an _____ is the actual occurrence of a threat.
a) Scam
b) Attack
c) Virus
d) Revenue loss

9. Place the attributes of an attack in order, from left to right:
a) Target (asset), Payload, Exploit, Attack vector, Vulnerability
b) Payload, Target (asset), Exploit, Attack vector, Vulnerability
c) Exploit, Vulnerability, Attack vector, Payload, Target (asset)
d) Attack vector, Exploit, Payload, Vulnerability, Target (asset)
e) Vulnerability
Attack Attributes (Question 9)

10. An _____ is made by human threat agent (or adversary), while a _____ is usually the result of an error, malfunction or mishap of some sort.
a) Security threat event, emergency event
b) Adversarial threat event, nonadversarial threat event
c) Nonadversarial threat event, adversarial

d) None of the above

11. Match the correct description with the column word (7 Marks)
Asset
Attack vector
Payload
Policies
Threat
Vulnerability
Cyberrisk
The core duty of cybersecurity is to identify, mitigate and manage _____ to an organization's digital assets.
2. A(n) _____ is anything capable of acting against an asset in a manner that can cause harm.
3. A(n) _____ is something of value worth protecting.
4. A(n) _____ is a weakness in the design, implementation, operation or internal controls in a process that could be exploited to violate the system security.
The path or route used to gain access to the target asset is known as a(n) _____ .
In an attack, the container that delivers the exploit to the target is called a(n) _____ .
_____ communicate required and prohibited activities and behaviors.

12. Match the correct description with the column word (7 Marks)
Patches
Rootkit
Standards
Guidelines
Policies
Identity management
Procedure
Malware
_____ is a class of malware that hides the existence of other malware by modifying the underlying operating system.
_____ provide details on how to comply with policies and standards.
_____ provide general guidance and recommendations on what to do in particular circumstances.
_____, also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations.
_____ are used to interpret policies in specific situations.
_____ are solutions to software programming and coding errors.
_____ includes many components such as directory services, authentication and authorization services, and user management capabilities such as provisioning and deprovisioning.

13. The following are all potential consequences of lack of confidentiality

except:
Disclosure of information protected by privacy laws
Legal action against the enterprise
Interference with national security
Fraud

14. The degree to which a user or program can create, modify, read, or write to a file is called:
Access control
File permission
Redundancy
Certification

15. Which information security component considers the level of sensitivity and legal requirements and is subject to change over time?
Integrity
Confidentiality
Availability
Authentication

16. Authentication is defined as which of the following? Select all that apply.
A system's ability to identify and differentiate between users
Users within an organization authorized to maintain and protect systems and networks
The act of verifying identity
The act of verifying a user's eligibility to access computerized information

17. Establishment and maintenance of user profiles that define the authentication, authorization and access controls for each user is called:
Privileged user management
Access rights
Identity management
Authentication

18. Which term describes a cryptology tool used to prove message integrity using algorithms to create unique numeric values?
Digital signatures
Hashes
Encryption
Access controls

19. The following are all potential consequences of lack of integrity except:
Inaccuracy
Erroneous decisions
Loss of productive time
Fraud

20. Integrity is described as:
Protection of information from unauthorized modification
Protection of information from unauthorized access or disclosure

Timely and reliable access to and use of information and systems
All of the above

21. Which of the following methods of control can help protect integrity? Select all that apply.
Logging
Digital Signatures
Hashes
Encryption

22. Which type of documentation records details of information or events in an organized record-keeping system, usually sequenced in the order in which they occurred?
Digital certificate
Digital signature
Log
Backup

23. A week of severe rainstorms has flooded your company's building. All servers have been ruined. It is estimated that business will be down for 3 weeks. This is an example of:
Lack of confidentiality
Lack of availability
Lack of integrity
All of the above

24. When two or more controls work in parallel to protect an asset, it is called:
Access control
Backup
Redundancy
Logging

25. Which of the following are types of backups?
Full, incremental and differential
Full, partial and differential
Full, incremental and variable
Full and differential

26. Which of the following describes a differential backup?
Only copies files that have changed since last full backup
Copies all files that have changed, regardless of last backup type
Copies every file in the system, regardless of last backup
None of the above

27. Potential consequences resulting from lack of availability include which of the following? Select all that apply.
Loss of functionality and operational effectiveness
Loss of productive time
Interference with enterprise’s objectives
Erroneous decisions

28. The concept that a message or other piece of information is genuine is called:
Integrity
Nonrepudiation
Confidentiality
Authentication

29. Which of the following describe authentication? Select all that apply.
The act of verifying identity
Verification of the correctness of a piece of data
A system’s ability to identify and differentiate between users
Designed to protect against fraudulent logon activity
Verifying a user's eligibility to access computerized information

30. Nonrepudiation is implemented through which of the following methods? Select all that apply.
Backups
Transactional logs
Digital signatures
Encryption

31. The process of converting plaintext messages, applying a mathematical function to them and producing ciphertext messages is called:
Encryption
Two factor authentication
Nonrepudiation
Cryptology

32. Which control mechanism defines authentication and authorization protocols for users?
Digital signature
Hashes
Access controls
File permissions