CyberRookie CSX Fundamentals - Mock Exam 4

Friday, September 13, 2019 3:00 PM

Section 4 - SECURITY OF NETWORKS, SYSTEMS, APPLICATIONS AND DATA

1. Place the correct term (left to right) in risk assessment methodology below:

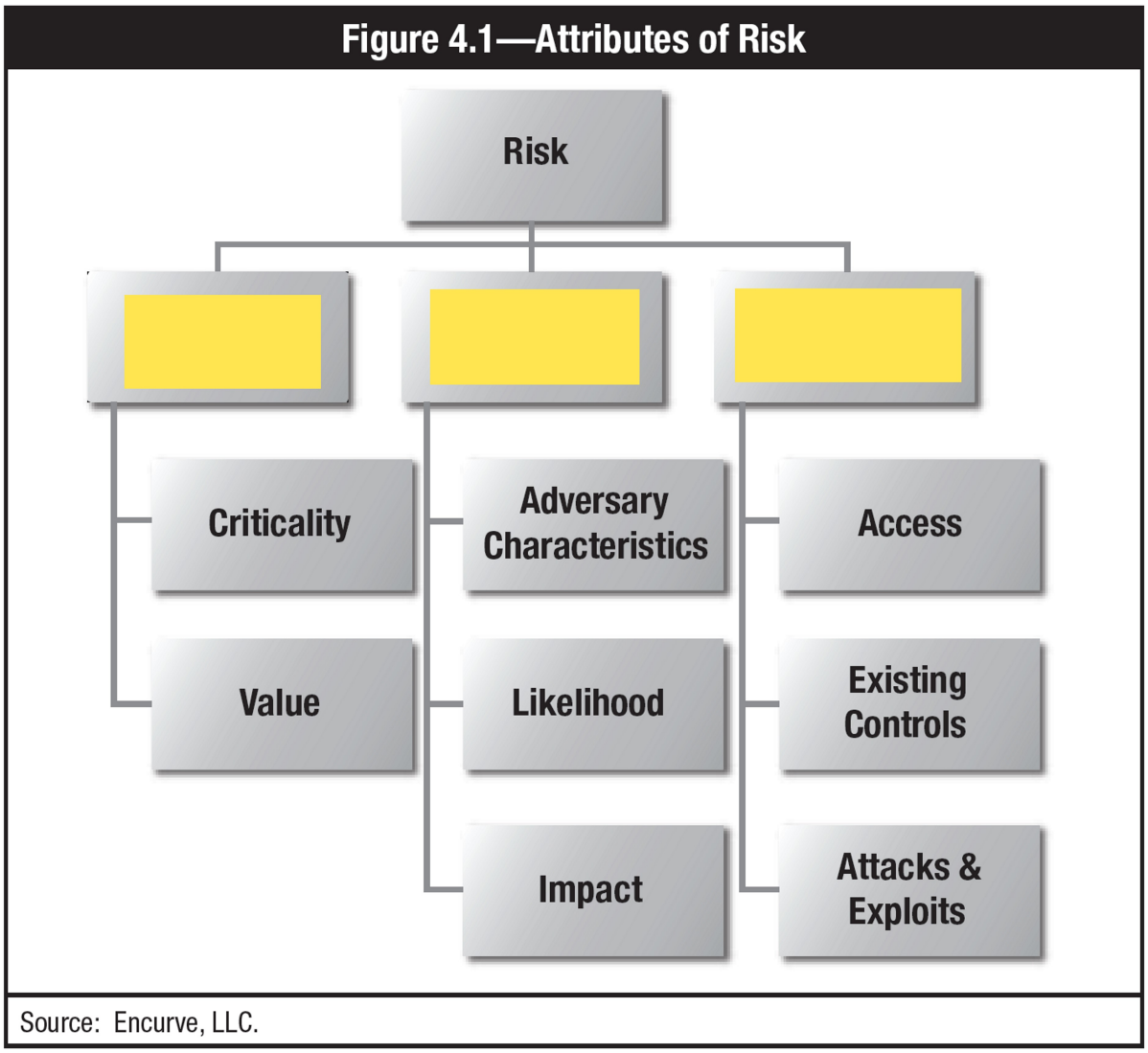
a) Assets, Threats, Vulnerabilities

b) Logs, Threats, Vulnerabiities, Assets

c) Threats, Logs, Vulnerabilites, Assests

d) Vulnerabilities, Assests, Logs, Threats

Attribute of Risk (Question 1)



2. These two inputs are used to collect data on assets, threats and vulnerabilities together and analyze them together to determine risk, _____ and _____.

a) Likelihoods, impacts

b) Logs, access-lists

c) Likes, dislikes

d) Employee experience, industry standards

3. Remediation means to:

a) Provide security solutions

b) Work with management

c) To protect digital asset

d) Mitigate or eliminate the vulnerability (such as patching)

4. Penetration testing common phases. Place the correct letter in blank spaces in the diagram.

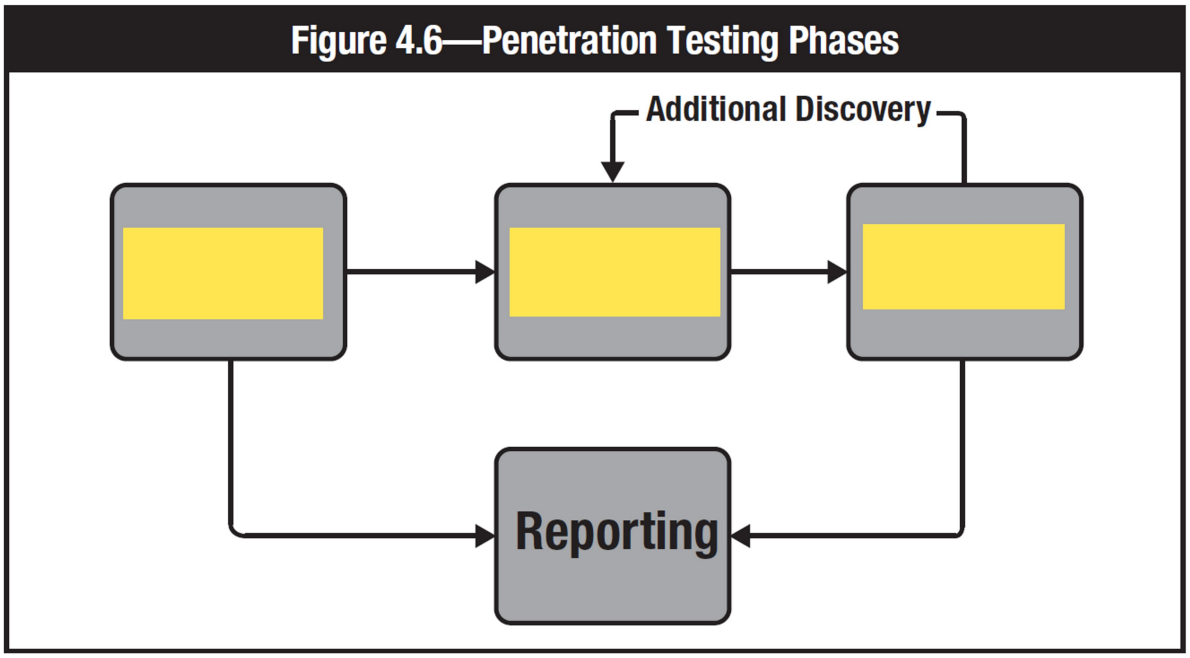
a) Planning, Discover, Attacks

b) Discovery, Planning, Logs

c) Attacks, Planning, Discovery

d) Logs, Planning, Attacks

Penetration Test Phase (Question 4)



5. Repeaters, hubs, Layer 2 switches, routers, Layer 3 & 4 switches are on premises _____ components in an organization.

a) LAN

b) WAN

c) MPLS

d) NAC

6. The aim of a NAC device is to:

a) Scan for unused ports

b) Monitor network traffic

c) Report security breaches

d) Control the access to a network using policies that describe how devices can secure access to network nodes when they first try to access the network.

7. Allowable ports numbers range from:

a) 0 to 65535

b) 0 to 1024

c) 0 to 2058

d) 0 to 85535

8. Ports reserved for certain privileged services:

a) 0 to 1023

b) 200 to 400

c) 0 to 10

d) 500 to 1000

9. This is an example of a Virtual Private Network (VPN):

a) Stealth network

b) Layer 10 tunneling

c) B2B

d) Point-to-point tunneling protocol (PPTP)

10. System hardening is the process of implementing:

a) A solid network

b) Cable assurance and connectivity

c) Ensuring the servers are well protected with a hard case

d) Security controls on a computer system

11. Graphic below is an example of what type of filesystem system:

a) UNIX

b) DOS

c) Windows

d) None of the above

Graphic for Question 11

- /etc/passwd—Maintains user account and password information
- /etc/shadow—Retains the encrypted password of the corresponding account
- /etc/group—Contains group information for each account
- /etc/gshadow—Contains secure group account information
- /bin—Location of executable files
- /boot—Contains files for booting system
- /kernel—Kernel files
- /sbin—Contains executables, often for administration
- /usr—Include administrative commands

12. Below is an example of _____ commands:

a) UNIX

b) DOS

c) Windows

d) None of the above

Graphic for Question 12

Figure 4.10— Commands

Command	Description
finger {userid}	Display information about a user
cat	Display or concatenate file
cd	Change directory
chmod	Change file permissions Note: UNIX permissions are managed using octal notation by user, group, and others. Manipulating permissions is above the purpose of this material but is critical as you further your cybersecurity career.
cp	Copy
date	Display current date and time
diff	Display differences between text files
grep	Find string in file

13. This technology allows multiple OSs (guests), to coexist on the same physical server (host), in isolation of one another:

a) Cohabit servers technology

b) Virtualization technology

c) Server integration technology

d) None of the above

14. Below is an example of what type of registry system:

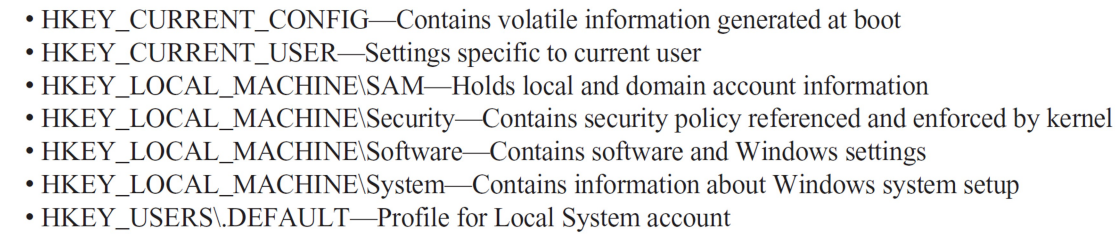
a) UNIX

b) DOS

c) Windows

d) None of the above

Graphic for Question 14



15. The system development life cycle includes these process, place them in the correct order:

a) Design -> Implementation ->Troubleshooting -> Planning

b) Implementation -> Troubleshooting -> Analysis -> Design

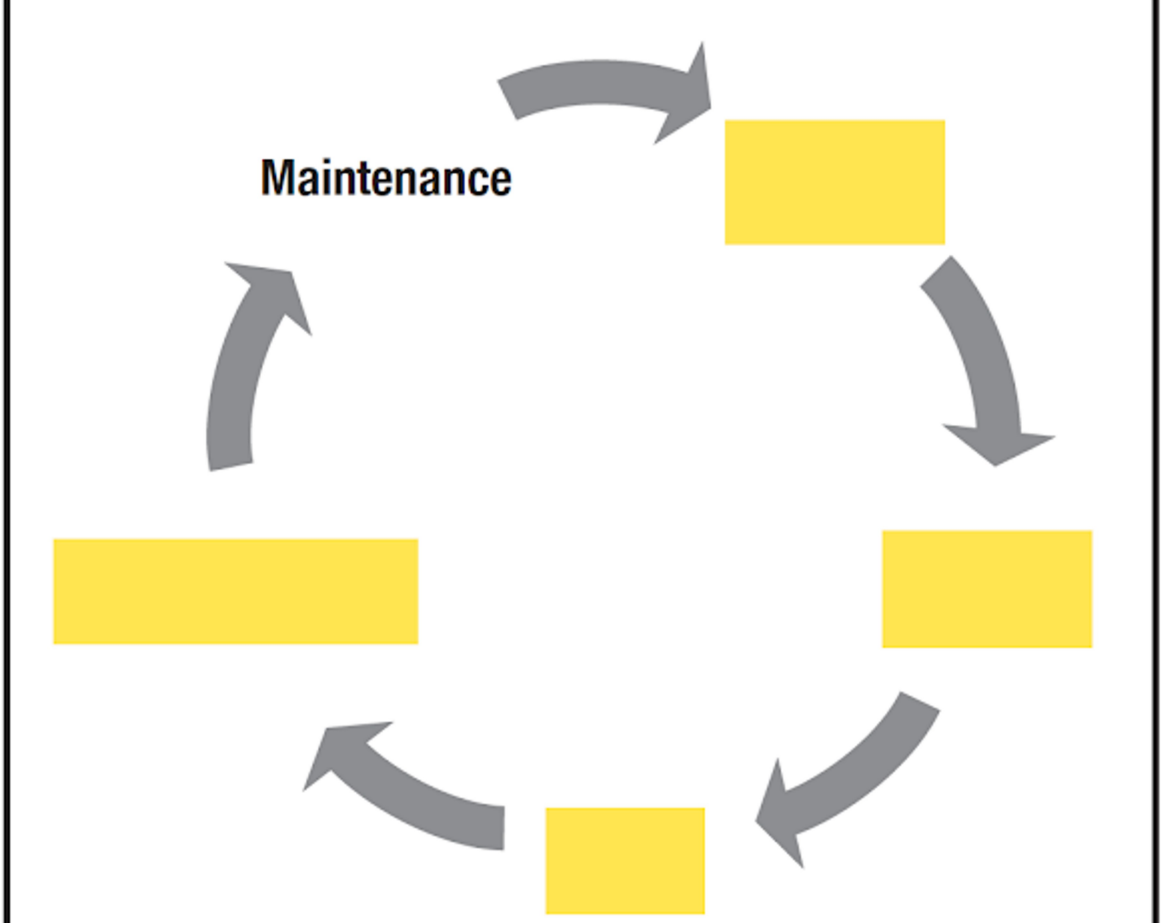
c) Troubleshooting -> Planning -> Analysis -> Design

d) Planning -> Analysis -> Design -> Implementation

e) Design ->Analysis -> Planning -> Implementation

Graphic for Question 15

Figure 4.12—SDLC Process



Source: National Institute of Standards and Technology (NIST), Special Publication (SP) 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*, USA, October 2008

17. Why is it important for an organization to classify its data

a) To keep it neat and tidy meeting LEED building certification and standards

b) It will quicken inspection from the CRA by allowing appropriate classification for indexing

c) Make the documentation managers happy

d) Allow the organization the capability to understand the sensitivity of information and classify data based on sensitivity and the impact of release or loss.

18. When classifying data, the following should be considered:

a) Confidentiality, privacy, access and authentication data retention, auditability, integrity

b) Confidentiality, process, access and authentication data retention, auditability, integrity

c) Classification, process, access and authentication data retention, auditability, integrity

d) The amount of data

19. After data classification has been assigned, security controls can be established such as:

a) Not needed

b) Backup, replication

c) Deduplication, offsite storage

d) Encryption, authentication and logging

20. Another important consideration for data security is to define:

a) The storage capacity

b) The database replication

c) The data owner

d) Cloud security

21. Put the steps of the penetration testing phase into the correct order.

A. Attack, Planning, Reporting, Discovey

B. Discovery, Reporting, Attack, Planning

C. Reporting, Attack, Discovery, Planning

D. Planning, Discovery, Attack, Reporting

22. System hardening should implement the principle of _____ or _____ .

A. Governance, compliance

B. Least privilege, access control

C. Stateful inspection, remote access

D. Vulnerability assessment, risk mitigation

23. Select all that apply. Which of the following are considered functional areas of network management as defined by ISO?

A. Accounting management

B. Fault management

C. Firewall management

D. Performance management

E. Security management

24. Virtualization involves:

A. the creation of a layer between physical and logical access controls.

B. multiple guests coexisting on the same server in isolation of one another.

C. simultaneous use of kernel mode and user mode.

D. DNS interrogation, WHOIS queries and network sniffing.

25. Vulnerability management begins with an understanding of cybersecurity assets and their locations, which can be accomplished by:

A. vulnerability scanning.

B. penetration testing.

C. maintaining an asset inventory.

D. using command line tools.

26. What is the main difference between a risk and a threat?

Risk involves the probability of an event and its consequence, a threat is anything that can cause harm

Risk involves determining weakness in design, a threat is anything that can cause harm

Risk is the combined action of a threat source with a threat event, a threat is the result of malicious activity

Risk is determined first, then potential threats are assessed

27. Risk assessment involves the analysis of:

Assets, threats and vulnerabilities

Risk tolerance, amount of data and scope of environment

Assets, threats and response

Risk response options, parameters and prioritization

28. People, information, infrastructure, finances and reputation are all considered:

Assets

Risks

Vulnerabilities

Threats

29. A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats is called a(n):

Asset

Vulnerability

Threat

Risk

30. All of the following are approaches to cybersecurity except:

Compliance-based

Ad hoc

Risk-based

Threat-based

31. After assets, threats and vulnerabilities have been assessed, risk can be rated based on:

Likelihood and impact

Threat events and threat source

Threat source and likelihood

Risk tolerance

32. The actual occurrence of a threat is called a(n):

Attack

Incident

Target

Event

33. Attack attributes include which of the following? Select all that apply.

Attack vector

Payload

Exploit

Vulnerability

Asset

34. Scanning the network perimeter, using open source discovery of organizational information and running malware to identify potential targets are activities that may be performed during which phase of the attack process?

Creating attack tools

Performing reconnaissance

Exploiting and compromising

Conducting an attack

35. Problems caused by aging equipment, natural disasters and mishandling of information by authorized users are all examples of:

Nonadversarial threats

Attack types

Risk attributes

Adversarial threats

36. The path or route used to gain access to a target (asset) is called a(n):

Attack vector

Exploit

Attack mechanism

Payload

37. Any method that is used to deliver an exploit is called a(n):

Attack mechanism

Attack vector

Payload

Vulnerability

38. All of the following are considered hostile threat agents except:

Script kiddies

Online social hackers

Hacktivists

Ethical hackers

39. Software designed to gain access to targeted computer systems, steal information or disrupt computer operations is called:

Malware

Botnet

Social engineering

Zero-day exploit

40. A piece of code that can replicate itself and spread from one computer to another is called a(n):

Virus

Trojan horse

Exploit

Rootkit

41. Spyware is a type of malware which:

Gathers information about a person or organization without the person’s or the organization’s knowledge

Locks or encrypts data or functions and demands a payment to unlock them

Secretly records user keystrokes and, in some cases, screen content

Hides the existence of other malware by modifying the underlying operating system

42. An attack made by trying all possible combinations of passwords or encryption keys until the correct one is found is called a(n):

Brute force attack

Botnet

SQL injection

Zero-day exploit

43. This variant of computer virus is a piece of self-replicating code designed to spread itself across computer networks:

Network worm

Trojan horse

Malware

Backdoor

Back

Next

Never submit passwords through Google Forms.