1) Who has the greatest influence over access security in a password authentication environment?

A. System administrators

B.Business executives

C.Users

D.Security managers

2) Which of the following interpret requirements and apply them to specific situations?

A. Policies

B.Standards

C.Guidelines

D.Procedures

3)Business continuity plans (BCPs) associated with organizational information systems should be developed primarily on the basis of:

A. Available resources

B.Levels of effort

C.Projected costs

D.Business needs

4)A segmented network:

A.Offers defense in depth superior to a concentric-layers model

B.Consists of two or more security zones

C.Maximizes the delay experienced by an attacker

D.Delivers superior performance for internal applications

5)Which cybersecurity principle is most important when attempting to trace the source of malicious activity?

A.Availability

B.Integrity

C.Nonrepudiation

D.Confidentiality

6)Which of the following offers the strongest protection for wireless network traffic?

A.Wireless Protected Access 2 (WPA2)

B.Wireless Protected Access-Advanced Encryption Standard (WPA-AES)

C.Wired Equivalent Protection 128-bit (WEP-128)

D.Wireless Protected Access-Temporary Key Integrity Protocol (WPA-TKIP)

7) Outsourcing poses the greatest risk to an organization when it involves:

A.Business support services

B.Technology infrastructure

C.Cybersecurity capabilities

D.Core business functions

8)Risk assessments should be performed:

A.At the start of a program

B.On a regular basis

C.When an asset changes

D.When a vulnerability is discovered

9)Maintaining a high degree of confidence regarding the integrity of evidence requires a(n):

A.Power of attorney

B.Sworn statement

C.Chain of custody

D.Affidavit

10)A firewall that tracks open connection-oriented protocol sessions is said to be:

A.State-sponsored

B.Stateless

C.Stateful

D.Stated

11)During which phase of the system development lifecycle (SDLC) should security first be considered?

A.Planning

B.Analysis

C.Design

D.Implementation

12)A cybersecurity architecture designed around the concept of a perimeter is said to be:

A.Data-centric

B.User-centric

C.Integrated

D.System-centric

13)A passive network hub operates at which layer of the OSI model?

A.Data Link

B.Physical

C.Network

D.Transport

14)Updates in cloud-computing environments can be rolled out quickly because the environment is:

A.Homogeneous

B.Distributed

C.Diversified

D.Secure

15)During which phase of the six-phase incident response model is the root cause determined?

A.Recovery

B.Identification

C.Containment

D.Eradication

16)The attack mechanism directed against a system is commonly called a(n):

A.Exploit

B.Vulnerability

C.Payload

D.Attack Vector

17)Where should an organization's network terminate virtual private network (VPN) tunnels?

A.At an interior router, to reduce network traffic congestion

B.At a dedicated "honey pot" system in the demilitarized zone (DMZ)

C.At the destination system, to prevent loss of confidentiality

D.At the perimeter, to allow for effective internal monitoring

18) In practical applications:

A.Symmetric key encryption is used to securely distribute asymmetric keys

B.Asymmetric key encryption is used to securely obtain symmetric keys

C.Symmetric key encryption is used only for short messages, such as digital signatures

D.Asymmetric key encryption is used in cases where speed is important

19) Which two factors are used to calculate the likelihood of an event?

A.Threat and vulnerability

B.Vulnerability and asset value

C.Asset count and asset value

D.Threat and asset count

20) What kind of anti-malware program evaluates system processes based on their observed behaviors?

A.Heuristic

B.Signature-based

C.Stateful

D.Polymorphic

21)A business continuity plan (BCP) is not complete unless it includes:

A.Dedicated resources

B.Detailed procedures

C.Network diagrams

D.Critical processes

22) Under the US-CERT model for incident categorization, a CAT-3 incident refers to which of the following?

A.Improper usage

B.Investigation

C.Denial of service (DoS)

D.Malicious code

23)An interoperability error is what type of vulnerability?

A.Technical

B.Process

C.Emergent

D.Organizational

24)Securing Supervisory Control and Data Acquisition (SCADA) systems can be challenging because they:

A.Operate in specialized environments and often have non-standard design elements

B.Are subject to specialized requirements established for national security systems

C.Support critical infrastructure processes for which any risk of compromise is unacceptable

D.Cannot be replaced due to aging infrastructure and the complexity of included components

25) Virtual systems should be managed using a dedicated virtual local area network (VLAN) because:

A.Network topologies do not always property identify the locations of virtual servers

B.VLAN encryption provides a double layer of protection for virtual system data

C.Insecure protocols could result in a compromise of privileged user credentials

D.Segregation of management traffic and use traffic dramatically improves performance