CEHv9 Exam Questions & Answers

Part 1 , 30 Questions (Question Number 1 to 30)

1. Which of the following is the BEST mitigation from phishing attacks?

- A. Network activity monitoring
- B. Security awareness training
- C. Corporate policy and procedures
- D. Strong file and directory permissions

Answer - B

2. What is the MOST effective countermeasure to a malicious code attack against a mobile system?

- A. Sandbox
- B. Change control
- C. Memory management
- D. Public-Key Infrastructure (PKI)

Answer - A

3. Which of the following is a physical security control that protects Automated Teller Machines (ATM) from skimming?

- A. Anti-tampering
- B. Secure card reader
- C. Radio Frequency (RF) scanner
- D.Intrusion Prevention System (IPS)

Answer - A

4. Which of the following is an essential element of a privileged identity life-cycle management?

- A. Regularly perform account re-validation and approval
- B. Account provisioning based on multi-factor authentication
- C. Frequently review performed activities and request justification
- D. Account information to be provided by supervisor or line manager

Answer - A

5. Which of the following is ensured when hashing files during chain of custody handling?

- A. Availability
- B. Accountability
- C. Integrity
- D. Non-repudiation

Answer - C

6. Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network
data leakage prevention and/or monitoring?

- A. Cross Origin Resource Sharing (CORS)
- B. Web-sockets

- C. Document Object Model (DOM) trees
- D. Web Interface Definition Language (IDL)

Answer - B

7. Which of the following statements is TRUE of black box testing?

- A. Only the functional specifications are known to the test planner.
- B. Only the source code and the design documents are known to the test planner.
- C. Only the source code and functional specifications are known to the test planner.
- D. Only the design documents and the functional specifications are known to the test planner.

Answer - A

8 . A software scanner identifies a region within a binary image having high entropy. What does this MOST likely indicate?

- A. Encryption routines
- B. Random number generator
- C. Obfuscated code
- D. Botnet command and control

Answer - C

9. Which of the following is a limitation of the Common Vulnerability Scoring System (CVSS) as it relates to conducting code review?

- A. It has normalized severity ratings.
- B. It has many worksheets and practices to implement.
- C. It aims to calculate the risk of published vulnerabilities.
- D. It requires a robust risk management framework to be put in place.

Answer - C

10. Which of the following is the MOST important consideration when storing and processing Personally Identifiable Information (PII)?

- A. Encrypt and hash all PII to avoid disclosure and tampering.
- B. Store PII for no more than one year.
- C. Avoid storing PII in a Cloud Service Provider.
- D. Adherence to collection limitation laws and regulations.

Answer - D

11. Which of the following assessment metrics is BEST used to understand a system's vulnerability to potential exploits?

- A. Determining the probability that the system functions safely during any time period
- B. Quantifying the system's available services
- C. Identifying the number of security flaws within the system
- D. measuring the system's integrity in the presence of failure

Answer - C

12. Which of the following is an effective method for avoiding magnetic media data remanence?

- A. Degaussing
- B. Encryption
- C. Data Loss Prevention (DLP)
- D. Authentication

Answer - A

13. Which of the following MUST be part of a contract to support electronic discovery of data stored in a cloud environment?

- A. Integration with organizational directory services for authentication
- B. Tokenization of data

- C. Accommodation of hybrid deployment models
- D. Identification of data location

Answer - D

14. When transmitting information over public networks, the decision to encrypt it should be based on

- A. the estimated monetary value of the information.
- B. whether there are transient nodes relaying the transmission.
- C. the level of confidentiality of the information.
- D. the volume of the information.

Answer - C

15. Logical access control programs are MOST effective when they are

- A. approved by external auditors.
- B. combined with security token technology.
- C. maintained by computer security officers.
- D. made part of the operating system.

Answer - D

16. What principle requires that changes to the plaintext affect many parts of the ciphertext?

- A. Diffusion
- B. Encapsulation
- C. Obfuscation
- D. Permutation

Answer - A

17. Which one of these risk factors would be the LEAST important consideration in choosing a building site for a new computer facility?

- A. Vulnerability to crime
- B. Adjacent buildings and businesses
- C. Proximity to an airline flight path
- D. Vulnerability to natural disasters

Answer - C

18. Which one of the following transmission media is MOST effective in preventing data interception?

- A. Microwave
- B. Twisted-pair
- C. Fiber optic
- D. Coaxial cable

Answer - C

19. Which security action should be taken FIRST when computer personnel are terminated from their
jobs?

- A. Remove their computer access.
- B. Require them to turn in their badge
- C. Conduct an exit interview
- D. Reduce their physical access level to the facility

Answer - A

20. A practice that permits the owner of a data object to grant other users access to that object would
usually provide

- A. Mandatory Access Control (MAC).

- B. owner-administered control.
- C. owner-dependent access control.
- D. Discretionary Access Control (DAC).

Answer - D

21. The type of authorized interactions a subject can have with an object is

- A. control.
- B. permission.
- C. procedure.
- D. protocol.

Answer - B

22. Why MUST a Kerberos server be well protected from unauthorized access?

- A. It contains the keys of all clients.
- B. It always operates at root privilege.
- C. It contains all the tickets for services.
- D. It contains the Internet Protocol (IP) address of all network entities.

Answer - A

23. Which one of the following effectively obscures network addresses from external exposure when
implemented on a firewall or router?

- A. Network Address Translation (NAT)
- B. Application Proxy
- C. Routing Information Protocol (RIP) Version 2
- D. Address Masking

Answer - A

24. While impersonating an Information Security Officer (ISO), an attacker obtains information from
company employees about their User IDs and passwords. Which method of information gathering
has the attacker used?

- A. Trusted path
- B. Malicious logic
- C. Social engineering
- D. Passive misuse

Answer - C

25. Why must all users be positively identified prior to using multi-user computers?

- A. To provide access to system privileges
- B. To provide access to the operating system
- C. To ensure that unauthorized persons cannot access the computers
- D. To ensure that management knows what users are currently logged on

Answer - C

26. The birthday attack is MOST effective against which one of the following cipher technologies?

- A. Chaining block encryption
- B. Asymmetric cryptography
- C. Cryptographic hash
- D. Streaming cryptography

Answer - C

27. Which one of the following is the MOST important in designing a biometric access system if it is
essential that no one other than authorized individuals are admitted?

- A. False Acceptance Rate (FAR)
- B. False Rejection Rate (FRR)
- C. Crossover Error Rate (CER)
- D. Rejection Error Rate

Answer - A

28. What is the term commonly used to refer to a technique of authenticating one machine to another
by forging packets from a trusted source?

- A. Man-in-the-Middle (MITM) attack
- B. Smurfing
- C. Session redirect
- D. Spoofing

Answer - D

29. The PRIMARY purpose of a security awareness program is to

- A. ensure that everyone understands the organization’s policies and procedures.
- B. communicate that access to information will be granted on a need-toknow basis.
- C. warn all users that access to all systems will be monitored on a daily basis.
- D. comply with regulations related to data and information protection.

Answer - A

30. As one component of a physical security system, an Electronic Access Control (EAC) token is best known for its ability to

- A. overcome the problems of key assignments.

- B. monitor the opening of windows and doors.
- C. trigger alarms when intruders are detected.
- D. lock down a facility during an emergency

Answer - A

Part 2 , 30 Questions (Question Number 31 to 60)

31. Which one of the following is a fundamental objective in handling an incident?

- A. To restore control of the affected systems
- B. To confiscate the suspect's computers
- C. To prosecute the attacker
- D. To perform full backups of the system

Answer - A

32. In the area of disaster planning and recovery, what strategy entails the presentation of information
about the plan?

- A. Communication
- B. Planning
- C. Recovery
- D. Escalation

Answer - A

33. The process of mutual authentication involves a computer system authenticating a user and
authenticating the

- A. user to the audit process.
- B. computer system to the user.

- C. user’s access to all authorized objects.
- D. computer system to the audit process.

Answer - B

34. What maintenance activity is responsible for defining, implementing, and testing updates to
application systems?

- A. Program change control
- B. Regression testing
- C. Export exception control
- D. User acceptance testing

Answer - A

35. Which one of the following describes granularity?

- A. Maximum number of entries available in an Access Control List (ACL)
- B. Fineness to which a trusted system can authenticate users
- C. Number of violations divided by the number of total accesses
- D. Fineness to which an access control system can be adjusted

Answer - D

36. In a basic SYN flood attack, what is the attacker attempting to achieve?

- A. Exceed the threshold limit of the connection queue for a given service
- B. Set the threshold to zero for a given service
- C. Cause the buffer to overflow, allowing root access
- D. Flush the register stack, allowing hijacking of the root account

Answer - A

37. The first step in building a firewall is to

- A. assign the roles and responsibilities of the firewall administrators.
- B. define the intended audience who will read the firewall policy.
- C. identify mechanisms to encourage compliance with the policy.
- D. perform a risk analysis to identify issues to be addressed.

Answer - D

38. A system has been scanned for vulnerabilities and has been found to contain a number of
communication ports that have been opened without authority. To which of the following might this
system have been subjected?

- A. Trojan horse
- B. Denial of Service (DoS)
- C. Spoofing
- D. Man-in-the-Middle (MITM)

Answer - A

39. Which type of control recognizes that a transaction amount is excessive in accordance with
corporate policy?

- A. Detection
- B. Prevention
- C. Investigation
- D. Correction

Answer - A

40. Which of the following defines the key exchange for Internet Protocol Security (IPSec)?

- A. Secure Sockets Layer (SSL) key exchange
- B. Internet Key Exchange (IKE)
- C. Security Key Exchange (SKE)
- D. Internet Control Message Protocol (ICMP)

Answer - B

41. The overall goal of a penetration test is to determine a system's

- A. ability to withstand an attack.
- B. capacity management.
- C. error recovery capabilities.
- D. reliability under stress.

Answer - A

42. When constructing an Information Protection Policy (IPP), it is important that the stated rules are
necessary, adequate, and

- A. flexible.
- B. confidential.
- C. focused.
- D. achievable.

Answer - D

43. Which one of the following affects the classification of data?

- A. Passage of time
- B. Assigned security label
- C. Multilevel Security (MLS) architecture
- D. Minimum query size

Answer - A

44. The Structured Query Language (SQL) implements Discretionary Access Controls (DAC) using

- A. INSERT and DELETE.
- B. GRANT and REVOKE.
- C. PUBLIC and PRIVATE.
- D. ROLLBACK and TERMINATE.

Answer - B

45. Which of the following is a network intrusion detection technique?

- A. Statistical anomaly
- B. Perimeter intrusion
- C. Port scanning
- D. Network spoofing

Answer - A

46. Internet Protocol (IP) source address spoofing is used to defeat

- A. address-based authentication.
- B. Address Resolution Protocol (ARP).
- C. Reverse Address Resolution Protocol (RARP).
- D. Transmission Control Protocol (TCP) hijacking.

Answer - A

47. Which of the following is an authentication protocol in which a new random number is generated
uniquely for each login session?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Point-to-Point Protocol (PPP)
- C. Extensible Authentication Protocol (EAP)
- D. Password Authentication Protocol (PAP)

Answer - A

48. What security management control is MOST often broken by collusion?

- A. Job rotation
- B. Separation of duties
- C. Least privilege model
- D. Increased monitoring

Answer - B

49. An Intrusion Detection System (IDS) is generating alarms that a user account has over 100 failed
login attempts per minute. A sniffer is placed on the network, and a variety of passwords for that
user are noted. Which of the following is MOST likely occurring?

- A dictionary attack
- B. A Denial of Service (DoS) attack
- C. A spoofing attack
- D. A backdoor installation

Answer - A

50. An engineer in a software company has created a virus creation tool. The tool can generate
thousands of polymorphic viruses. The engineer is planning to use the tool in a controlled
environment to test the company’s next generation virus scanning software. Which would best
describe the behavior of the engineer and why?

- A. The behavior is ethical because the tool will be used to create a better virus scanner.
- B. The behavior is ethical because any experienced programmer could create such a tool.
- C. The behavior is not ethical because creating any kind of virus is bad.
- D. The behavior is not ethical because such a tool could be leaked on the Internet.

Answer - A

51. Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?

- A. Hot site
- B. Cold site
- C. Warm site
- D. Mobile site

Answer - B

52. Which of the following statements is TRUE for point-to-point microwave transmissions?

- A. They are not subject to interception due to encryption.
- B. Interception only depends on signal strength.
- C. They are too highly multiplexed for meaningful interception.
- D. They are subject to interception by an antenna within proximity.

Answer - D

53. The key benefits of a signed and encrypted e-mail include

- A. confidentiality, authentication, and authorization.
- B. confidentiality, non-repudiation, and authentication.
- C. non-repudiation, authorization, and authentication.
- D. non-repudiation, confidentiality, and authorization.

Answer - B

54. If only the sender and the receiver can see data because it is hidden in a graphic or media, this is an example of using what method of concealment?

- A. Encryption bit
- B. Steganography
- C. One-time password
- D. Transposition cipher

Answer - B

55. What NMAP flag is used for OS Detection?

- A. -S
- B. -T
- C. -O
- D. -Pn

Answer - C

56. The Privacy Act legislates how personal identifiable information can be used collected and distributed?

- A. True
- B. False

Answer - A

57. In regards to information security, what is confidentiality?

- A. Making sure data is accessible when permitted parties request it.
- B. When data can only be accessed by permitted parties.
- C. Making sure unauthorized changes are not made to data.

- D. When data is genuine and not corrupted.

Answer - B

58. Which of the following circumstances is most effectively mitigated by using data mirroring?

- A. The recovery point objective is high.
- B. The recovery point objective (RPO) is low.
- C. The recovery time objective (RTO) is high.
- D. Disaster tolerance is high.

Answer - B

59. In regards to information security, what is availability?

- A. Making sure data is accessible when permitted parties request it.
- B. When data is genuine and not corrupted.
- C. When data can only be accessed by permitted parties.
- D. Making sure unauthorized changes are not made to data.

Answer - A

60. SNMP is a network management protocol that is usually set up to use UDP instead of TCP packets? (True or False)

- A. True
- B. False

Answer - A

Part 3 , 40 Questions (Question Number 61 to 100)

61. A company user uses his personal phone for the majority of his business phone calls. He has been advised by management that he is required to shred his phone bill before throwing it in the trash. Which of the following is the company attempting to avoid.

- A. Shoulder surfing
- B. Dumpster diving
- C. Eavesdropping
- D. Data extraction

Answer - B

62. Systems that ethical hackers attack with no knowledge of its configuration is

- A. Black Box
- B. White Box
- C. Grey Box
- D. Know Box

Answer - A

63. Flooding a web service using a lot of infected clients (botnet) to bring down it's performance is called:

- A. DDoS
- B. Sniffing
- C. Buffer Overflow
- D. DoS
- E. LOIC

Answer - A

64. When an ethical hacker is working in the Gaining Access phase, which one of the following attack types takes advantage of built in scripts that off-theshelf applications often include?

- A. Misconfiguration attacks
- B. Application-level attacks
- C. Shrink-wrap code attacks
- D. DDoS attacks

Answer - C

65. In regards to information security, what is confidentiality?

- A. Making sure unauthorized changes are not made to data.
- B. Making sure data is accessible when permitted parties request it.
- C. When data is genuine and not corrupted.
- D. When data can only be accessed by permitted parties.

Answer - D

66. A computer threat that tries to exploit computer application vulnerabilities that are unknown to others and undisclosed to the software developer is a(n):

- A. Attack
- B. Exploit
- C. Target
- D. Zero-Day Vulnerability

Answer - D

67. In regards to information security, what is availability?

- A. Making sure unauthorized changes are not made to data.
- B. When data is genuine and not corrupted.

- C. Making sure data is accessible when permitted parties request it.
- D. When data can only be accessed by permitted parties.

Answer - C

68. When do you need approval from a customer to perform penetration testing on their systems?

- A. When you are attempting to access sensitive data
- B. When you are about to test a privilege escalation exploit
- C. Always
- D. Every time you are using illegal tools

Answer - C

69. __ is a Linux utility commonly used to crack passwords.

- A. ROT13
- B. NTLM
- C. Elliptic-Curve
- D. Cicada
- E. John the Ripper
- F. All of the above

Answer - E

70. The program snow is used for:

- A. Password attacks
- B. Spyware
- C. Steganography
- D. Sniffing

Answer - C

71. Information may be hidden into the slack space of a file.

- A. True
- B. False

Answer - A

72. What software can be used to alter an image in stenography?

- A. Photoshop
- B. Firefox
- C. Explorer
- D. S-Tools

Answer - A

73. ________replaces unneeded bits in an image and sound files with secret data.

- A. Steganography
- B. Tempest
- C. Forensics
- D. Cryptography

Answer - A

74. Any text that one can imagine can be hidden inside an image.

- A. True
- B. False

Answer - A

75. What is steganography?

- A. A cryptographic technique that uses exclusively analog technology which predates computing.
- B. A method of using rainbow tables in order to crack encryption.
- C. A method of hiding data in another media type in order to conceal it.
- D. A method of designing PKI systems.

Answer - C

76. It is possible to hide a text message in _.

- A. All of these
- B. A graphic file
- C. An audio file
- D. Another message

Answer - A

77. Steganography is used by:

- A. Artists/Owners
- B. All of these
- C. Hackers
- D. Terrorists

Answer - B

78. Steganography can be used for legitimate purposes.

- A. True
- B. False

Answer - A

79. LSB insertion can serve as a steganographic technique to hide messages in audio files.

- A. True
- B. False

Answer - A

80. Steganography can be used to pass messages through uploaded photos on Facebook.

True or False?

- A. True
- B. False

Answer - A

81. Secret communications where the existence of the message is hidden is known as .

- A. Concealment Cipher
- B. Image Processing
- C. Running Cipher
- D. Steganography

Answer - D

82. Lossless compression are considered best for those applications where the integrity of an original information can be maintained. True or false?

- A. True
- B. False

Answer - A

83. Steganography can be detected by certain programs.

- A. True
- B. False

Answer - A

84. The term that is best described as a process of replacing unwanted bits in an image and its source files with the secret data is known as .

- A. Forensic Analysis
- B. Steganography
- C. Network Analysis
- D. Cryptography

Answer - B

85. Which of these is a potential carrier file?

- A. All of these
- B. Executable file
- C. Audio file
- D. Image file

Answer - A

86. Which of the layered approaches to security hides data in ICMP traffic:

- A. Covert channels
- B. Unique
- C. Hiding directories
- D. Encryption

Answer - A

87. Which of the following represents a form of steganography technique?

- A. Password protection
- B. Encryption
- C. Highlight
- D. Digital watermarking

Answer - D

88. Which form of steganography generally includes a replication of an image so that any document source can be authenticated in a partial manner?

- A. BMP tagging
- B. Time stamp
- C. Digital watermarking
- D. Date stamp

Answer - C

89. JPEG images use discrete cosine transformation to achieve an optimal compression.

True or false?

- A. True
- B. False

Answer - A

90. The color of every 50th pixel in a video file corresponds to a letter in the alphabet. This is an example of steganography.

- A. True
- B. False

Answer - A

91. True or false, Steganalysis detection performance is specified by the receiver operating characteristic or OC curve. The Operating Characteristic (OC) curve is the probability of detection versus the cumulative distribution.

- A. True
- B. False

Answer - A

92. In steganography, it is crucial that only those people who are expecting the message know the message exists.

- A. True
- B. False

Answer - A

93. True or false, lossless compression is better suited to applications where the integrity of the original information must be maintained?

- A. True
- B. False

Answer - A

94. Which of the following bit size images provides the most hiding space for information?

- A. Single bit
- B. 16-bit
- C. 24-bit
- D. 8-bit

Answer - C

95. Which of the following are three primary colors that are normally used in image analysis?

- A. Peach, yellow, pink
- B. Brown, red, orange
- C. Red, green, blue,
- D. Black, white, gray

Answer - C

96. Which of these is used during steganography to withstand statistical steganalysis?

- A. Stream-based cryptography process
- B. Data whitening process
- C. Data encoding process
- D. All of these

Answer - D

97. A stego is sent as a secret information that is embedded in normal traffic. Which of the following method is used?

- A. Hidden active directory
- B. Punching
- C. Encryption
- D. Covert channels

Answer - D

98. Which process uses a GIF and BMP file that allows software to exactly reconstruct an original image?

- A. Lost
- B. Lossless
- C. Laid compression
- D. Waste-less

Answer - B

99. Of these answers, which best describes the art of steganography?

- A. The act of scrambling data using complex algorithms and special keys in order to secure and conceal data.
- B. A malicious act where an insider-threat uses encryption and compression to smuggle data from a secured network
- C. The process by which programmers break down and analyze code that is encrypted.
- D. The process of injecting or concealing secret data or code into a common, easily-readable file so that the secret cannot be easily detected by ordinary means.

Answer - D

100. Which of the following is the main use of digital watermarks and digital fingerprinting?

- A. Monitoring patent applications
- B. Track copyright issues
- C. Develop a covert communication
- D. Enhance duplication

Answer - B