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

Part 4 , 30 Questions (Question Number 101 to 130)

101. What are noisy areas in steganography realm?

- A. Grayscale color area
- B. Black areas
- C. Areas with a great deal of natural color variation
- D. Areas with little color variation

Answer - C

102. The tool 'snow' is a steganography tool.

- A. whitespace
- B. blackspace
- C. deep
- D. deadspace

Answer - A

103. Adding identifiable information into a file or document is known as .

- A. Copyright hiding
- B. Counterfeiting
- C. Watermarking
- D. None of these

Answer - C

104. True or false stenography's niche in security of information is to replace cryptography?

- A. True
- B. False

Answer - B

105. The study of discovering messages that were hidden using the process of steganography is known as .

- A. None of these
- B. Steganographics
- C. Steganographism
- D. Steganalysis

Answer - D

106. Steganography that is using a carrier chain would fail to reconstruct a message when:

- A. Any of these
- B. A carrier is modified
- C. Carriers are processed in the wrong order
- D. A carrier is unavailable

Answer - A

107. True or false. The robustness of spread spectrum steganography against active text comes at the cost of low and embedding capacity.

- A. True
- B. False

Answer - A

108. Steganalysis is not the method that is used to detect stenography.

- A. True
- B. False

Answer - B

109. Which of the following methods would help best in preventing the malicious steganography?

- A. Routine server analysis
- B. Specialized training
- C. Hiring of internal developers
- D. Policy that restricts installation of unauthorized programs on company's computers

Answer - D

110. True or false the properties of single files and entire directories can be changed to a hidden status to hide messages using the stego process?

- A. True
- B. False

Answer - A

111. Traffic security can be correctly categorized under:

- A. Traffic intelligence
- B. Electric intelligence
- C. Electronic security
- D. Communication security

Answer - D

112. Steganography noticeably changes the carrier file.

- A. True
- B. False

Answer - B

113. Which of the following activities is(are) considered to be anti-forensics?

- A. Data sanitizing
- B. Trail obfuscation
- C. Artifact wiping
- D. Data hiding
- E. All of the above

Answer - E

114. How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?

- A. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options.
- B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions.
- C. Performing common services for the application process and replacing real applications with fake ones.
- D. Defeating the scanner from detecting any code change at the kernel.

Answer - A

115. Which of these rootkits would you rate as the most effective?

- A. Kernel level
- B. Application level
- C. Physical level
- D. Library level

Answer - A

116. Rootkits are harder to detect than other malware.

- A. True
- B. False

Answer - A

117. A rootkit is capable of:

- A. Hiding processes
- B. Hiding registry keys
- C. All of these
- D. Hiding files

Answer - C

118. Rootkits are for:

- A. Multiplying and slowing a system down
- B. Sending out mass quantities of traffic
- C. Providing covert access to the machine over long periods of time
- E. Generating revenue from ads

Answer - C

119. Rootkits are capable of modifying all existing software, including the ones that are designed to circumvent it.

- A. True
- B. False

Answer - A

120. A Trojan can contain a rootkit. True or false?

- A. True
- B. False

Answer - A

121. What is a rootkit?

- A. It's malware that intercepts packets in transit without being stored onto a target machine
- B. It's malware that propagates without a specific target
- C. It's malware that's used to gain access to a computer or computer system while being undetected
- D. It's malware that uses social engineering techniques

Answer - C

122. You are doing a pen test against an organization that has just recovered from a major cyber-attack. The CISO and CIO want to completely and totally eliminate risk. What is one of the first things you should explain to these individuals?

- A. Explain that you cannot eliminate all risk but you will be able to reduce risk to acceptable levels.
- B. Explain to them that they need to buy more services.
- C. Tell him everything is going to a ok and collect that check!
- D. Start the Wireshark application to sniff traffic

Answer - A

123. What should you do if a friend asks you to perform and penetration test as a favor outside your normal job of being a pen tester for a consulting company?

- A. Start the test immediately
- B. Start foot printing the friend's network
- C. Start social engineering the friends company
- D. Ask your employer for permission to perform the test outside of your normal work

Answer - D

124. Which solution can be used to emulate real services such as ftp, mail, etc and capture login attempts and related information? They're often used to study hacker's activities.

- A. Layer 4 switch
- B. Core server
- C. Honeypot
- D. Firewall

Answer - C

125. You need to monitor all traffic on your local network for suspicious activity and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

- A. Host based IDS
- B. Proxy
- C. Network based IDS
- D. Firewall

Answer - C

126. Which property or concept ensures that a hash function will not produce the same hashed value for two different messages?

- A. Key strength
- B. Entropy
- C. Bit length
- D. Collision resistance

Answer - D

127. What is this Shellshock bash vulnerability attempting to do on this vulnerable Linux host?

env x='(){:;};echo exploit' bash -c 'cat /etc/passwd'

- A. Change all password in passwd
- B. Remove the passwd file.
- C. Add new user to the passwd file
- D. Display passwd contents to prompt

Answer - D

128. During a routine assessment you discover information that suggests the customer is involved in human trafficking.

- A. Ignore the data complete the job collect a check. Keep it moving!
- B. Immediately stop work and contact the proper legal authorities
- C. Copy the data to a thumb drive and keep it as leverage.
- D. Confront the client in a respectful manner and ask about the data

Answer - B

129. What is the best description of SQL Injection?

- A. It is an attack used to modify the code in an application
- B. It is a Denial of Service Attack (DoS)
- C. It is a MiTM attack
- D. It is an attack used to gain unauthorized access to a database

Answer - D

130. Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

- A. The root CA stores the user's hash value for safekeeping.
- B. The root CA is the recovery agent used to encrypt data when a user's certificate is lost
- C. The root CA is used to encrypt email messages to prevent unintended disclosure of data
- D. The CA is the trusted root that issues certificates

Answer - D

Part 5 , 30 Questions (Question Number 131 to 160)

131. What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

- A. Impact Risk
- B. Inherent Risk
- C. Deferred Risk

- D. Residual Risk

Answer - D

132. Which of the following problems can be solved by using Wireshark?

- A. Resetting the administrator password on multiple systems
- B. Troubleshooting communication resets between two systems
- C. Tracking version changes of source code
- D. Checking creation dates on all webpages on a server

Answer - B

133. This kind of malware is installed by criminals on your computer so they can lock it from a remote location. This malware generates a popup window, webpage, or email warning from what looks like an official authority such as the FBI.It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again. Which term best matches this definition?

- A. Ransomware
- B. Adware
- C. Riskware
- D. Spyware

Answer - A

134. Which of the following is a hashing algorithm?

- A. DES
- B. PGP
- C. ROT13
- D. MD5

Answer - D

135. An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to
be entered. This is an example of what kind of software design problem/issue?

- A. Insufficient firewall rules
- B. Insufficient input validation
- C. Insufficient exception handling
- D. Insufficient anti-virus detection

Answer - B

136. What is the best way to defend against network sniffing?

- A. Register all machines MAC address in a Centralized Database and
- B. limit network connection to those machines
- C. Use Static IP's
- D. Using encryption protocols on network communications
- E. Restrict physical access to server rooms host critical servers

Answer - D

137. What is a collision attack in cryptography?

- A. Collision attacks try to break the hash into two parts with the same bytes in each part to get the private key
- B. Collision attacks try to get the public key
- C. Collision attacks try to find two inputs that produce the same hash
- D. Collision attacks try to break the hash into three parts.

Answer - C

138. Which of the following is an example of the principle of least privilege as a system security control?

- A. User should have limited access to the information regardless of its purpose
- B. User must be able to access only the information and resources that are necessary for legitimate purpose
- C. User should access all the information stored in the business to best execute their functions
- D. Companies should have only a few employees

Answer - B

139. Which tool queries publicly available databases that contain domain name registration contact information?

- A. netstat
- B. ifconfig
- C. WHOIS
- D. Nslookup

Answer - C

140. The TJ Max breach happened in part because this type of weak wireless security was implemented.

- A. WiFi Protected Access (WPA)
- B. TKIP
- C. Wired Equivalent Privacy (WEP)
- D. WPA2

Answer - C

141. Which wireless hacking tool attacks WEP and WPA-PSK?

- A. Airguard

- B. wificracker
- C. Aircrack-ng
- D. WLAN-crack

Answer - C

142. Which of the following techniques will identify if computer files have been changed?

- A. Network sniffing
- B. Integrity checking hashes
- C. Firewall alerts
- D. Permissions sets

Answer - B

143. Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack.Stuxnet attack was an unprecedented style of attack because it used four types of this vulnerability. What is this style of attack called?

- A. zero-sum
- B. zero-day
- C. no-day
- D. zero-hour

Answer - B

144. An individual who aims to bring down critical infrastructure for a "cause" and is not worried about facing 30 years in jail for their action.

- A. Black Hat
- B. Suicide Hacker
- C. Gray Hat

- D. White Hat

Answer - B

145. During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

- A. Terminate the audit
- B. Identify and evaluate existing practices
- C. Create a procedures document
- D. Conduct compliance testing

Answer - B

146. As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing. What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

- A. Project Scope
- B. Rules of Engagement
- C. Service Level Agreement
- D. Non-disclosure Agreement

Answer - B

147. An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up. What is the most likely cause?

- A. The attacker altered or erased events from the logs.
- B. Proper chain of custody was not observed while collecting the logs.
- C. The security breach was a false positive.
- D. The network devices are not all synchronized.

Answer - A

148. While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country.
The email asks the user to call his bank and verify the authorization of a funds transfer that took
place. What Web browser-based security vulnerability was exploited to compromise the user?

- A. Web form input validation
- B. Cross-Site Request Forgery
- C. Clickjacking
- D. Cross-Site Scripting

Answer - B

149. This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like.
What is the most important phase of ethical hacking in which you need to spend a considerable
amount of time?

- A. Gaining access
- B. Escalating privileges
- C. Network mapping
- D. Footprinting

Answer - D

150. Which of the following is a command line packet analyzer similar to GUI- based Wireshark?

- A. Ethereal
- B. Nessus

- C. Tcpdump
- D. John the ripper

Answer - C

151. Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

- A. SOA
- B. Biometrics
- C. PKI
- D. Single sign on

Answer - C

152. Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

- A. Containment phase
- B. Recovery phase
- C. Identification phase
- D. Preparation phase

Answer - D

153. Which of the following is a protocol specifically designed for transporting event messages?

- A. ICMP
- B. SMS
- C. RDP
- D. SYSLOG

Answer - D

154. You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?
alert tcp any any -> 192.168.100.0/24 21 (msg: ""FTP on the network!"";)

- A. FTP Server rule
- B. A Router IPTable
- C. An Intrusion Detection System
- D. A firewall IPTable

Answer - C

155. You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

- A. Piggybacking
- B. Social engineering
- C. Tailgating
- D. Eavesdropping

Answer - B

156. An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.
<iframe
rc="http://www.vulnweb.com/updateif.php"style="display:none"></iframe>
What is this type of attack (that can use either HTTP GET or HTTP POST) called?

- A. SQL Injection
- B. Cross-Site Scripting

- C. Browser Hacking
- D. Cross-Site Request Forgery

Answer - B

157. Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?

- A. Service Oriented Architecture
- B. Agile Process
- C. Lean Coding
- D. Object Oriented Architecture

Answer - A

158. After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first?

- A. Disable Key Services
- B. Create User Account
- C. Disable IPTables
- D. Download and Install Netcat

Answer - D

159. This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach. Which of the following organizations is being described?

- A. International Security Industry Organization (ISIO)
- B. Payment Card Industry (PCI)
- C. Institute of Electrical and Electronics Engineers (IEEE)
- D. Center for Disease Control (CDC)

Answer - B

160. What is the process of logging, recording, and resolving events that take place in an organization?

- A. Security Policy
- B. Internal Procedure
- C. Incident Management Process
- D. Metrics

Answer - C

Part 6 , 40 Questions (Question Number 161 to 200)

161. env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'
What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

- A. Display passwd content to prompt
- B. Changes all passwords in passwd
- C. Add new user to the passwd file
- D. Removes the passwd file

Answer - A

162. You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms
when needed. What type of alert is the IDS giving?

- A. True Positive
- B. True Negative
- C. False Negative
- D. False Positive

Answer - C

163. What does a firewall check to prevent particular ports and applications from getting packets into an organization?

- A. Application layer port numbers and the transport layer headers
- B. Transport layer port numbers and application layer headers
- C. Presentation layer headers and the session layer port numbers
- D. Network layer headers and the session layer port numbers

Answer - B

164. When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if
using web vulnerability scanners. What proxy tool will help you find web vulnerabilities?

- A. Burpsuite
- B. Proxy chains
- C. Dimitry
- D. Maskgen

Answer - A

165. You have successfully gained access to your client's internal network and successfully comprised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled. Which port would you see listening on these Windows machines in the network?

- A. 1433
- B. 161
- C. 3389
- D. 445

Answer - D

166. Which of the following is a component of a risk assessment?

- A. Administrative safeguards
- B. Logical interface
- C. DMZ
- D. Physical security

Answer - A

167. Using Windows CMD, how would an attacker list all the shares to which the current user context has access?

- A. NET FILE
- B. NET USE
- C. NET VIEW
- D. NET CONFIG

Answer - C

168. Perspective clients want to see sample reports from previous penetration tests. What should you do next?

- A. Decline, just provide the details of the components that will be there in the report.
- B. Share full reports, not redacted.
- C. Decline, just provide references.
- D. Share sample reports with redactions after NDA is signed.

Answer - A

169. Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any

information besides the company name. What should be the first step in security testing the client?

- A. Scanning
- B. Enumeration
- C. Escalation
- D. Reconnaissance

Answer - D

170. The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?

- A. Cross Site Scripting
- B. Cross Site Request Forgery
- C. Injection
- D. Path disclosure

Answer - C

171. Which regulation defines security and privacy controls for Federal information systems and organizations?

- A. EU Safe Harbor
- B. PCI-DSS
- C. HIPAA
- D. NIST-800-53

Answer - D

172. When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation. What command will help you to search files using Google as a search engine?

- A. inurl: target.com filename:xls username password email
- B. site: target.com filetype:xls username password email site:
- C. target.com file:xls username password email domain:
- D. target.com archive:xls username password email

Answer - B

173. You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS). What is the best way to evade the NIDS?

- A. Out of band signaling
- B. Alternate Data Streams
- C. Protocol Isolation
- D. Encryption

Answer - D

174. Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very Difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

- A. Burpsuite
- B. Hydra
- C. Whisker
- D. TCP splice

Answer - C

175. It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure. Which of the following regulations best matches the description?

- A. ISO/IEC 27002
- B. HIPAA
- C. FISMA
- D. COBIT

Answer - B

176. Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

- A. ESP transport mode
- B. AH Tunnel mode
- C. ESP confidential
- D. AH promiscuous

Answer - A

177. A regional bank hires your company to perform a security assessment on Their network after a recent data breach. The attacker was able to steal Financial data from the bank by compromising only a single server. Based On this information, what should be one of your key recommendations to
The bank?

- A. Require all employees to change their anti-virus program with a New one
- B. Move the financial data to another server on the same IP Subnet
- C. Issue new certificates to the web servers from the root certificate Authority
- D. Place a front-end web server in a demilitarized zone that Only handles external web traffic

Answer - D

178. Which of the following is one of the most effective ways to prevent Cross- site Scripting (XSS) flaws in software applications?

- A. Use digital certificates to authenticate a server prior to Sending data
- B. Use security policies and procedures to define and Implement proper security settings

- C. Validate and escape all information sent to a server
- D. Verify access right before allowing access to protected Information and UI controls

Answer - C

179. You are the Systems Administrator for a large corporate organization. You Need to monitor all network traffic on your local network for suspicious Activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

- A. Firewall
- B. Proxy
- C. Network-based IDS
- D. Host-based IDS

Answer - C

180. In 2007, this wireless security algorithm was rendered useless by Capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft Through a technique known as war driving. Which Algorithm is this Referring to?

- A. Wi-Fi Protected Access 2 (WPA2)
- B. Wi-Fi Protected Access (WPA)
- C. Temporal Key Integrity Protocol (TKIP)
- D. Wired Equivalent Privacy (WEP)

Answer - D

181. Which of the following tools can be used for passive OS fingerprinting?

- A. tracert
- B. ping
- C. nmap
- D. tcpdump

Answer - A

182. You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed.
You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run Wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

- A. tcp.dstport==514 && ip.dst==192.168.0.99
- B. tcp.srcport==514 && ip.src==192.168.150
- C. tcp.dstport==514 && ip.dst==192.168.0.150
- D. tcp.srcport==514 && ip.src==192.168.0.99

Answer - C

183. You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System. What is the best approach?

- A. Install and use Telnet to encrypt all outgoing traffic from this server.
- B. Use Alternate Data Streams to hide the outgoing packets from this server.
- C. Install Cryptcat and encrypt outgoing packets from this server.
- D. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

Answer - C

184. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems. The security concept of "separation of duties" is most similar to the operation of which type of security device?

- A. Bastion host
- B. Honeypot
- C. Firewall

- D. Intrusion Detection System

Answer - A

185. An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to
be entered. This is an example of what kind of software design problem?

- A. Insufficient security management
- B. Insufficient exception handling
- C. Insufficient database hardening
- D. Insufficient input validation

Answer - D

186. Which of the following is not a Bluetooth attack?

- A. Bluedriving
- B. Bluesmacking
- C. Bluesnarfing
- D. Bluejacking

Answer - A

187. A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

- A. The client cannot see the SSID of the wireless network
- B. The WAP does not recognize the client's MAC address
- C. The wireless client is not configured to use DHCP
- D. Client is configured for the wrong channel

Answer - C

188. The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk.
It will require a further 4 hours to restore the database from the last backup to the new hard disk. The
recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).
What is the closest approximate cost of this replacement and recovery operation per year?

- A. $146
- B. $440
- C. $100
- D. $1320

Answer - A

Solution: ((300 +140) *1) /3

189. Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a Linux platform?

- A. Kismet
- B. Netstumbler
- C. Nessus
- D. Abel

Answer - A

190. To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

- A. Intrusion Detection System
- B. Protocol analyzer

- C. Vulnerability scanner
- D. Port scanner

Answer - C

191. What is a "Collision attack" in cryptography?

- A. Collision attacks try to get the public key
- B. Collision attacks try to find two inputs producing the same hash.
- C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.
- D. Collision attacks try to break the hash into three parts to get the plaintext value.

Answer - B

192. Which of the following is the greatest threat posed by backups?

- A. A backup is incomplete because no verification was performed
- B. A backup is unavailable during disaster recovery
- C. A backup is the source of Malware or illicit information.
- D. An un-encrypted backup can be misplaced or stolen

Answer - D

193. A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

- A. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.
- B. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
- C. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.

- D. Attempts by attackers to access the user and password information stored in the company's SQL database.

Answer - C

194. You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.
invictus@victim_server:
~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx.
QUITTING!
What seems to be wrong?

- A. OS Scan requires root privileges.
- B. The nmap syntax is wrong.
- C. This is a common behavior for a corrupted nmap application.
- D. The outgoing TCP/IP fingerprinting is blocked by the host firewall.

Answer - A

195. During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network. What is this type of DNS configuration commonly called?

- A. Split DNS
- B. DNSSEC
- C. DNS Scheme
- D. DynDNS

Answer - A

196. It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it

and demands payment before you can access your files and programs again. Which of the following terms best matches the definition?

- A. Ransomware
- B. Spyware
- C. Riskware
- D. Adware

Answer - A

197. Which of these options is the most secure procedure for storing backup tapes?

- A. In a cool dry environment
- B. In a climate controlled facility offsite
- C. Inside the data center for faster retrieval in a fireproof safe
- D. On a different floor in the same building

Answer - B

198. Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

- A. Wireshark
- B. Cain & Abel
- C. Maltego
- D. Metasploit

Answer - C

199. Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

- A. Dsniff
- B. John the Ripper

- C. Snort
- D. Nikto

Answer - D

200. Which of the following describes the characteristics of a Boot Sector Virus?

- A. Overwrites the original MBR and only executes the new virus Code
- B. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
- C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
- D. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

Answer - C