**SIT182 Introduction to Computer Security**

**Examination**

**Trimester 2, 2016**

**Special Instructions**

This examination is CLOSED BOOK.

Calculators are NOT ALLOWED.

Writing time is 2 HOURS.

This examination comprises **TWO** sections (A and B) and constitutes **50%** of your assessment in this unit.

**Section A** -**20 marks** contains 40 multiple choice questions. Please answer all questions on the Multiple Choice Answer Sheet provided. Choose the alternative which best answers the question and fill in the corresponding response circle completely.

**Section B – 30 marks** contains **6** short answer questions. The marks for each question carries are given accordingly.

Attempt **all questions**.

Ensure you write your Student Identification Number, Seat number, Unit Code and Location Code in the boxes provided at the top of the sheet.

**This examination question booklet must be handed in with any used**

**answer booklets and your multiple choice answer sheet.**

**SECTION A**

1. **What is the first step in addressing issues with passwords?**
2. The first step in addressing password issues is to create an effective and manageable password policy that both system administrators and users can work with.
3. The first step in addressing password issues is to find a systematic, alpha-numeric combination and then assign passwords, so that both system administrators and users can tell which department is using what system.
4. The first step in addressing password issues is to see how many passwords are required.
5. The first step in addressing password issues is to see how many accounts can use the same password.
6. **A network administrator wants to specify the number of days a password must be used before it can be changed again. What domain password policy will need to be configured?**
7. Enforce password history
8. Maximum password age
9. Minimum password age
10. Minimum password length
11. **The access control model that most closely resembles an organization's structure is:**
12. MAC
13. DAC
14. RBAC
15. RBOC
16. **What is the name of the process that controls access to information based on the sensitivity of that information and whether or not the user is operating at the appropriate sensitivity level and has the authority to access that information?**
17. MAC
18. DAC
19. RBAC
20. RBOC
21. **Why is wireless problematic from a security standpoint?**
22. There is no control over physical limitations.
23. Insufficient signal strength
24. There is no control over the physical layer of traffic.
25. There is no control over the network.
26. **Agents intercept a message that is encrypted. They use various techniques to try and decipher the plain text message. This is an example of**
27. Desteganographying
28. Decrypting
29. Uncrypting
30. Cryptanalysis
31. **A virtual private network (VPN) is a construct used to provide**
32. Users with their own web space on the network
33. An area of relaxation for employees
34. Secure communication channel between users across public networks such as the Internet
35. A learning area for programming languages
36. **Simple rule sets that are applied to port number and IP addresses are called**
37. Network address translation
38. Stateful packet filtering
39. Access control lists
40. Basic packet filtering
41. **The buffer between the outer network where there are no controls and the inner secure network is referred to as the**
42. DMZ
43. Intranet
44. Extranet
45. Internet
46. **How does stateful packet filtering differ from basic packet filtering?**
47. Stateful packet filtering looks only at each packet individually.
48. Stateful packet filtering looks at the packets in relation to other packets.
49. Stateful packet filtering looks at the destination address.
50. Stateful packet filtering looks at the source address.
51. **Encrypting a message by simply rearranging the order of the letters is a function of the**
52. Shift cipher
53. Substitution cipher
54. Transposition cipher
55. Vigenère cipher
56. **When users are unable to access information or the systems processing information, you may have suffered a**
57. Loss of confidentiality
58. Loss of integrity
59. Loss of authentication
60. Loss of availability
61. **Keyspace refers to**
62. The location where keys are stored
63. The number of keys needed to encrypt or decrypt a message
64. All possible key values
65. The portion of the algorithm that the key connects with to encrypt or decrypt a message
66. **On a UNIX system, if a file has the permission rwx r-- ---, what permission does the group have?**
67. Execute, read, write
68. Read
69. Read, write, execute
70. No permissions
71. **The correct sequence of the three-way handshake is**
72. SYN/SYN, ACK/ACK, SYN/SYN
73. SYN/ACK, SYN/ACK, SYN/ACK
74. SYN, SYN/ACK, ACK
75. ACK, SYN/ACK, SYN
76. **The first step an administrator can take to reduce possible attacks is to**
77. Ensure all patches for the operating system and applications are installed
78. Install a firewall
79. Install anti-spyware software
80. Configure an intrusion detection system
81. **Your boss would like you to implement a network device that will monitor traffic and turn off processes and reconfigure permissions as necessary. To do this you would use**
82. A firewall
83. A sniffer
84. A passive HIDS
85. An active HIDS
86. **Linux and other operating systems use the \_\_\_\_\_\_\_ command to change the read-write-execute properties of a file or directory.**
87. tracert
88. ifconfig
89. chmod
90. chkconfig
91. **Cryptographic algorithms are used for all of the following EXCEPT:**
92. Confidentiality
93. Integrity
94. Availability
95. Authentication
96. **What is an unstructured threat?**
97. An elite hacker who mounts an attack against a specific target
98. A poorly engineered building
99. A type of malicious code that formats the hard drive on a computer.
100. An attack that is uncoordinated, nonspecific, and lasts a short amount of time
101. **A buffer overflow can best be described as**
102. A hacker who makes a website that has more content than the browser can handle
103. A hacker who sends more data than is expected in an attempt to overwrite legitimate memory
104. A hacker who uses an e-mail virus to format the hard drive with junk code
105. A hacker who sends repeated requests for information from a server in an attempt to crash the server
106. **A newly purchased server with a defect catches fire and all data on the device is lost. A backup was never performed. This is a failure of which element of the operational model of computer security?**
107. Protection
108. Prevention
109. Detection
110. Response
111. **Securing e-mail is something that must be done by**
112. Networking administrators
113. Security administrators
114. Outlook express
115. Users
116. **The main purpose of a honeypot is**
117. To identify hackers so they can be tracked down by the FBI
118. To slow hackers down by providing an additional layer of security that they must pass before accessing the actual network
119. To distract hackers away from attacking an organization's live network
120. To help security professionals better understand and protect against threats to the system
121. **The SFTP protocol incorporates what into FTP?**
122. SSL
123. Secure java scripting
124. 28bit encryption key
125. the TCP protocol
126. **When a message sent by a user is digitally signed with a private key, the person will not be able to deny sending the message. This application of encryption is an example of copy of an encryption key with a trusted third party is known as**
127. Authentication
128. Nonrepudiation
129. Confidentiality
130. Auditing
131. **Malicious code that is scripted to send itself to other users is known as a \_\_\_\_\_\_\_\_.**
132. virus
133. worm
134. Trojan
135. logic bomb
136. **Multifactor authentication is all of these, EXCEPT:**
137. What you are
138. What you have
139. What you know
140. What you calculate
141. **Making data look like it has come from a different source is called**
142. Sniffing
143. A man-in-the-middle attack
144. A replay attack
145. Spoofing
146. **Bob connects to a company web site. His browser indicates that the digital certificate of the web site is valid. This application of encryption is an example of**
147. Authentication
148. Nonrepudiation
149. Integrity
150. Confidentiality
151. **Selecting a good password for each user account is critical to protecting information systems. How should you select a good password?**
152. Use letters in your first name and letters in your last name.
153. Select a password that is still relatively easy to remember, but still difficult to "guess."
154. Unfortunately, there is way to keep a password safe, so it really doesn't matter what you use.
155. Create a password that would be hard to remember, and then write it down so you won't forget it.
156. **What is the process of establishing a system's security state called?**
157. Hardening
158. Baselining
159. Securing
160. Controlling
161. **The primary vulnerability associated with many methods of remote access is**
162. Weak encryption
163. Too complicated for users to understand
164. The passing of critical data in clear text
165. Incompatibility with firewalls
166. **Locks, sign-in logs, and security guards are examples of**
167. Access controls.
168. Intrusion detection mechanisms.
169. Authentication methods.
170. Auditing devices.
171. **How can the purpose of risk management best be described?**
172. A method to improve the performance of the organizations stock portfolio
173. To take cost effective measures to reduce potential risk to the organization to an acceptable level
174. A method to inform management of the types of assets the company controls
175. A means of getting cheaper insurance for the organization
176. **Which of the following describes the process of asset identification during a risk assessment?**
177. Collecting data on the value of bank accounts and other financial notes controlled by the organization
178. Identifying and classifying the assets, systems, and processes that need protection because they are vulnerable to threats
179. Collecting data on the property plant and equipment to be prepared to file an insurance claim
180. Hiring an outside auditing firm to assess the total net worth of the company
181. **Contract management, fraud, regulatory risk management, and business continuity management are examples of**
182. Business risks
183. Technology risks
184. Market risks
185. Operational risks
186. **Which of the following is the value for the number of times an event is expected to occur in a year?**
187. SLE
188. ALE
189. SRO
190. ARO
191. **Which of the following is the formula for single loss expectancy (SLE)?**
192. The exposure factor added to the asset
193. The asset multiplied by the exposure factor
194. The asset divided by the annual rate of expectancy
195. The asset multiplied by the exposure factor and divided by the annual rate of expectancy
196. **What are the steps for the software engineering institute model for risk management?**
197. Identify, analyze, plan, track, and control
198. Analyze, track, identify, plan, and control
199. Identify assets, threats, vulnerabilities, and exposure factor
200. Cost benefit analysis, control, and review

**SECTION B (30 marks)**

1. What is Cryptanalysis? **(2 marks)**
2. Explain the difference between social engineering and reverse social engineering. **(4 marks)**
3. Describe the **three** basic types of network topologies and provide a simple diagram of each type topology. **(6 marks)**
4. Describe the following methods of access management: **(8 marks)**
5. Mandatory access control
6. Discretionary access control
7. Role-based access control
8. Rule-based access control
9. Explain the asymmetric encryption and its advantages and disadvantages. **(5 marks)**
10. Explain the differences between Quantitative and Qualitative risk management. **(5 marks)**

**END OF EXAMINATION**