**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 process used to ensure that users have the correct rights to perform their jobs?**
17. Usage auditing
18. Audit trails
19. Privilege auditing
20. Escalation auditing
21. **A corporate spy copies proprietary information into a text file and then hides the text file in an image file. The image file is then posted on the company's web site for others who know where to look to extract the information. This is the example of the use of**
22. Social engineering
23. Steganography
24. Cryptography
25. Cryptanalysis
26. **Multifactor authentication is all of these, EXCEPT:**
27. What you are
28. What you have
29. What you know
30. What you calculate
31. **When users are unable to access information or the systems processing information, you may have suffered a**
32. Loss of confidentiality
33. Loss of integrity
34. Loss of authentication
35. Loss of availability
36. **What is the process of establishing a system's security state called?**
37. Hardening
38. Baselining
39. Securing
40. Controlling
41. **What is an unstructured threat?**
42. An elite hacker who mounts an attack against a specific target
43. A poorly engineered building
44. A type of malicious code that formats the hard drive on a computer.
45. An attack that is uncoordinated, nonspecific, and lasts a short amount of time
46. **Locks, sign-in logs, and security guards are examples of**
47. Access controls.
48. Intrusion detection mechanisms.
49. Authentication methods.
50. Auditing devices.
51. **Which of the following is NOT a disadvantage of host-based IDS?**
52. The IDS uses local system resources.
53. The IDS can have a high cost of ownership and maintenance.
54. The IDS must have a process on every system you want to watch.
55. The IDS is ineffective when traffic is encrypted.
56. **The cipher that replaces each letter of the alphabet with a different letter (not in sequence) is a**
57. Shift cipher
58. Substitution cipher
59. Transposition cipher
60. Vigenère cipher
61. **What is a good first step for companies to take to fight potential social engineering attacks?**
62. Buy the latest virus protection software and install on the systems
63. Establish policies and procedures dictating the roles and responsibilities all users, as well as security administrators
64. Monitor all phone calls
65. Conduct background checks on all contractors, consultants, delivery persons, and partners that may have access to the facilities
66. **With the RSA and Diffie-Hellman handshakes**
67. The server and the client agree on what type of browser to use.
68. Parameters are agreed upon and certificates and keys are exchanged.
69. Parameters are agreed upon so that java scripts cannot execute inside the client system.
70. Office applications are able to e-mail secure documents.
71. **Keyspace refers to**
72. The location where keys are stored
73. The number of keys needed to encrypt or decrypt a message
74. All possible key values
75. The portion of the algorithm that the key connects with to encrypt or decrypt a message
76. **The SFTP protocol incorporates what into FTP?**
77. SSL
78. Secure java scripting
79. 28bit encryption key
80. the TCP protocol
81. **The main purpose of a honeypot is**
82. To identify hackers so they can be tracked down by the FBI
83. To slow hackers down by providing an additional layer of security that they must pass before accessing the actual network
84. To distract hackers away from attacking an organization's live network
85. To help security professionals better understand and protect against threats to the system
86. **The correct sequence of the three-way handshake is**
87. SYN/SYN, ACK/ACK, SYN/SYN
88. SYN/ACK, SYN/ACK, SYN/ACK
89. SYN, SYN/ACK, ACK
90. ACK, SYN/ACK, SYN
91. **Which of the following in a browser guarantees perfect security?**
92. SSL/TLS
93. SSH
94. Secure java scripting
95. There is no guarantee of perfect security.
96. **Which of the following should a password NOT contain?**
97. Eight or more characters
98. Dictionary words
99. At least one uppercase and one lowercase letter
100. At least one number and one special character or punctuation mark
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. **The buffer between the outer network where there are no controls and the inner secure network is referred to as the**
107. DMZ
108. Intranet
109. Extranet
110. Internet
111. **The encryption method based on the idea of two keys, one that is public and one that is private is**
112. Hashing function
113. Symmetric encryption
114. Asymmetric encryption
115. Elliptical curve encryption
116. **A virtual private network (VPN) is a construct used to provide**
117. Users with their own web space on the network
118. An area of relaxation for employees
119. Secure communication channel between users across public networks such as the Internet
120. A learning area for programming languages
121. **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**
122. A firewall
123. A sniffer
124. A passive HIDS
125. An active HIDS
126. **Keeping a copy of an encryption key with a trusted third party is known as**
127. CYA
128. Key escrow
129. Key redundancy
130. Key management
131. **\_\_\_\_\_\_\_\_\_ is sending an unauthorized message to another bluetooth device.**
132. Bluejacking
133. Bluesnarfing
134. Bluehacking
135. Bluephreaking
136. **The primary vulnerability associated with many methods of remote access is**
137. Weak encryption
138. Too complicated for users to understand
139. The passing of critical data in clear text
140. Incompatibility with firewalls
141. **How does stateful packet filtering differ from basic packet filtering?**
142. Stateful packet filtering looks only at each packet individually.
143. Stateful packet filtering looks at the packets in relation to other packets.
144. Stateful packet filtering looks at the destination address.
145. Stateful packet filtering looks at the source address.
146. **Making data look like it has come from a different source is called**
147. Sniffing
148. A man-in-the-middle attack
149. A replay attack
150. Spoofing
151. **Malicious code that is scripted to send itself to other users is known as a \_\_\_\_\_\_\_\_.**
152. virus
153. worm
154. Trojan
155. logic bomb
156. **Simple rule sets that are applied to port number and IP addresses are called**
157. Network address translation
158. Stateful packet filtering
159. Access control lists
160. Basic packet filtering
161. **Why is wireless problematic from a security standpoint?**
162. There is no control over physical limitations.
163. Insufficient signal strength
164. There is no control over the physical layer of traffic.
165. There is no control over the network.
166. **Securing e-mail is something that must be done by**
167. Networking administrators
168. Security administrators
169. Outlook express
170. Users
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. **Which of the following is used to calculate the threshold for evaluating the cost/benefit ratio of a given countermeasure?**
182. SLE
183. ALE
184. SRO
185. ARO
186. **What is the formula for annual rate of expectancy?**
187. The asset multiplied by the exposure factor
188. The exposure factor added to the asset
189. The single loss expectancy multiplied by the annual rate of occurrence
190. The asset divided by the annual rate of expectancy
191. **What are the steps for the software engineering institute model for risk management?**
192. Identify, analyze, plan, track, and control
193. Analyze, track, identify, plan, and control
194. Identify assets, threats, vulnerabilities, and exposure factor
195. Cost benefit analysis, control, and review
196. **Risk management is most often**
197. Purely qualitative
198. Purely quantitative
199. Both qualitative and quantitative
200. Purely objective

**SECTION B (30 marks)**

1. Describe the **three** basic types of network topologies and provide a simple diagram of each type topology. **(6 marks)**
2. Explain the difference between social engineering and reverse social engineering. **(4 marks**)
3. What is Cryptanalysis? **(2 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. Describe what a Virtual Private Network (VPN) is and what benefits it provides users.

**(5 marks)**

1. Explain the differences between Symmetric cryptography and asymmetric cryptography.**(5 marks)**

**END OF EXAMINATION**