Вопросы итогового контроля
по предмету “Безопасность операционных систем с открытым кодом”

1. Понятие и назначение операционных систем.
2. Понятие безопасности операционных систем с открытым кодом.
3. Классификация угроз безопасности операционной системы.
4. Атаки на операционные системы с открытым кодом.
5. Понятие защищенной операционной системы.
6. Подходы к созданию защищенных операционных систем.
7. Стратегия безопасности операционных систем.
8. Атаки на операционные системы. Классификация злоумышленников.
9. Направления и методы реализации угроз информационной безопасности.
10. Фрагментарный подход к созданию операционных систем.
11. Комплексный подход к созданию операционных систем.
12. Атаки на ОС: сканирование файловой системы.
13. Атаки на ОС: кража ключевой информации.
14. Атаки на ОС: атаки класса «отказ в обслуживании».
15. Атаки на ОС: подбор пароля и сборка мусора.
16. Безопасность процессов и потоков.
17. Многозадачный режим работы ОС с открытым кодом. Типы многозадачности.
18. Состояния процессов в ОС: действие, готовность, блокировка.
19. Создание и завершение процессов в ОС с открытым кодом.
20. Классическая модель потоков в ОС с открытым кодом.
21. Взаимосвязь между заданиями, процессами и потоками в операционных системах.
22. Реализация потоков в пользовательском пространстве.
23. Реализация потоков в ядре.
24. Управление процессами и потоками в ОС с открытым кодом.
25. Управление памятью в ОС с открытым кодом.
26. Методы управления памятью в операционных системах.
27. Пейджинг и фрагментация.
28. Внутренняя и внешняя фрагментация.
29. Понятия динамического связывания и динамической загрузки.
30. Статическая и динамическая загрузка.
31. Статическое и динамическое связывание.
32. Управление памятью в Linux.
33. Управление памятью: виртуальная память.
34. Управление памятью: физическая память.
35. Исполнение и загрузка пользовательских программ в ОС с открытым кодом.
36. Безопасность обмена данными и связи.
37. Моделирование угроз ОС. Методология DREAD.
38. Моделирование угроз ОС. Методология STRIDE.
39. Безопасный запуск операционной системы (Secure Boot).
40. Безопасность обмена данными и связи: концепции безопасности.
41. Безопасность файловых систем: Ext4.
42. Безопасность файловых систем: Btrfs.
43. Безопасность файловых систем: XFS.
44. Перспективы безопасности ОС с открытым кодом.
45. Основные направления развития операционных систем.

46. Программные средства для обеспечения безопасности операционной системы Linux.
47. Создаются ли домашние каталоги учётных записей пользователей при их добавлении с использованием команд adduser и useradd?
48. Какими способами можно добавить или удалить учётную запись пользователя из группы?
49. Какая утилита используется для модификации учётных записей пользователей?
50. Что определяет атрибуты файлов и каким образом их можно просмотреть и изменить?
51. Какие методы создания и удаления файлов, каталогов Вы знаете?
52. В чем заключается поиск по шаблону?,
53. Дайте определение понятий гетерогенная сеть и интерфейс.
54. Дайте определение понятий протокол, сокет и дуплекс.
55. Дайте определение понятий сокет, физический адрес, логический адрес, коммутатор.
56. Дайте определение понятий гетерогенная сеть, дуплекс, физический адрес, логический адрес.
57. Каково назначение пакета *iproute*2?
58. В чем основное назначение *пакета net-tools*?
59. Какими командами осуществляется проверка и управление характеристиками сетевых интерфейсов?
60. Какие утилиты включает в себя пакет *iproute*2?
61. Значение команд при работе с ОС Linux: history –c, who [am i], cal [[месяц]год], cat <имя файла>, cat text.1 > text.2, cat > text.1, rm <имя файла>, wc [имя файла], mkdir <имена создаваемых каталогов>, rmdir <имена удаляемых каталогов>, pwd, clear, exit.
62. Типы файловых систем, их предназначение и отличия.
63. Распространённые атаки на операционные системы.
64. Программные средства обеспечения безопасности информационных ресурсов.
65. Использование средств криптографической защиты информации (СКЗИ) в ОС с открытым кодом.
66. Сравнение операционных систем с открытым исходными кодом и проприетарных ОС: преимущества и недостатки.
67. Что представляет собой подсистема защиты операционной системы при применении фрагментарного подхода?
68. Основные составляющие стратегии безопасности операционных систем.
69. Уязвимости операционных систем с открытым кодом.
70. Атаки нацеленные на полный или частичный вывод операционной системы из строя.
71. Типы многозадачности ОС.
72. Виды состояния процесса в ОС. Приведите примеры.
73. В каком состоянии процесс может быть заблокирован в связи с внешними причинами, по инициативе операционной системы? Приведите примеры.
74. Как называется состояние, при котором процесс заблокирован и не может выполняться по своим внутренним причинам? Приведите примеры.
75. Зачем необходим процесс управления памятью в рамках функционирования ОС?
76. В каком случае ядро создает новое виртуальное адресное пространство?
77. Резидентная память и ее использование в ОС с открытым кодом?
78. Что является ловушкой обращения памяти? Приведите примеры.
79. По каким признакам можно классифицировать существующие системы защиты программного обеспечения?
80. Дайте определения данных типов алгоритмов: алгоритмы шифрования данных, алгоритмы запутывания, алгоритмы мутации, алгоритмы сжатия данных.

81. Каковы положительные стороны систем парольной защиты при процессе аутентификации пользователей в ОС?
82. Характерные особенности процесса протоколирования и аудита.
83. Понятие активного аудита в операционной системе.
84. Функциональные компоненты активного аудита.
85. Основные задачи протоколирования и аудита в ОС.
86. Какие операционные системы с открытым кодом используются в мобильных устройствах? В чем их особенности?
87. В чем заключаются различия процессов дефрагментации и фрагментации?
88. Что Вы знаете о такой атаке как «сборка мусора»?
89. Преимущества и недостатки операционных систем с открытым кодом.
90. Какие варианты реализации ядра в операционных система Вы знаете?
91. Что такое многозадачность и какие ее типы Вы знаете?
92. В чем заключается необходимость проведения аудита при работе с операционными системами?
93. Приведите описание каждой из атак представленных в методологии STRIDE.
94. Что такое журналирование и какова роль данного процесса в обеспечении информационной безопасности?
95. Распространенные атаки на ОС: бэкдоры и их преимущества.
96. Интерактивный вход в операционную систему. Методы аутентификации: локальный вход и доменный вход (Active Directory).
97. Программные и аппаратные средства защиты операционных систем.
98. Объясните роль тестирования на проникновение при оценке уровня защищенности операционных систем.
99. Какова роль информационных форумов и почтовых рассылок при разработке и сопровождении приложений с открытым исходным кодом?
100. Функциональные компоненты и архитектура средств активного аудита.
101. Разведка по открытым источникам open source intelligence (OSINT).
102. Выявление уязвимостей с помощью передовых технологий написания сценариев.
103. Функция ядра операционной системы.
104. Характерные особенности Linux как операционной системы.
105. Распространенные уязвимости и угрозы в системах Linux.
106. Распространённые проблемы безопасности в конфигурации Linux.
107. Вредоносное программное обеспечение и компрометация операционных систем. Вымогатели.
108. Вредоносное программное обеспечение и компрометация операционных систем. Криптомайнеры.
109. Вредоносное программное обеспечение и компрометация операционных систем. Руткиты.
110. Вредоносное программное обеспечение и компрометация операционных систем. Черви.
111. Вредоносное программное обеспечение и компрометация операционных систем. Бэкдоры.
112. Вредоносное программное обеспечение и компрометация операционных систем. Трояны удалённого доступа (RAT).
113. Способы шифрования пароля в операционной системе Linux.
114. Шифрование информации в операционной системе Linux.
115. Шифрование файла с помощью ключей в операционной системе Linux.

116. Шифрование файла с помощью пароля в операционной системе Linux.
117. Инструменты для шифрования и дешифрования файлов защищенных паролем.
118. Процесс сканирования в операционной системе Linux.
119. Инструменты для сканирования систем и сетей в операционной системе Linux.
120. Методы сканирования систем и сетей.
121. Методы сканирования систем и сетей. Сетевые сканеры.
122. Методы сканирования систем и сетей. Веб-сканеры.
123. Методы сканирования систем и сетей. Сканеры программного обеспечения.
124. Концепция процессов и потоков. Задания, процессы, потоки (нити), волокна.
125. Безопасность процессов и потоков в операционных системах. Конкуренция процессов в борьбе за ресурсы.
126. Способ организации файловой системы в операционных системах с открытым кодом.
127. Сетевая безопасность системы Linux.
128. Сетевая безопасность системы Linux: использование надежных паролей.
129. Сетевая безопасность системы Linux: включение двухфакторной аутентификации.
130. Сетевая безопасность системы Linux: настройка и включение брандмауэра.
131. Сетевая безопасность системы Linux: регулярный мониторинг журналов и системной активности.
132. Основные компоненты среды Linux.
133. Программные средства для обеспечения безопасности операционных систем.
134. Обнаружение внутрисетевых угроз: на основе хоста - Host-based (HIDS).
135. Обнаружение внутрисетевых угроз: на основе сети - Network-based (NIDS).
136. Обнаружение внутрисетевых угроз. Threat Hunting в Linux.
137. Устранение распространенных проблем безопасности.
138. Основные категории инструментов безопасности. Инструменты сетевой безопасности.
139. Основные категории инструментов безопасности. Инструменты оценки уязвимостей.
140. Основные категории инструментов безопасности. Инструменты шифрования и аутентификации.
141. Основные методы диагностики распространенных проблем безопасности: анализ журналов.
142. Основные методы диагностики распространенных проблем безопасности: мониторинг системных ресурсов.
143. Расширенные стратегии диагностики: профилирование производительности.
144. Распространенные проблемы с инструментами безопасности. Проблемы с конфигурацией брандмауэра.
145. Распространенные проблемы с инструментами безопасности. Ошибки аутентификации.
146. Распространенные проблемы с инструментами безопасности. Устранение неполадок в инструментах сетевой безопасности.
147. Типичные угрозы безопасности операционной системы мобильного устройства.
148. Безопасность мобильных операционных систем.
149. Проблемы обеспечения безопасности операционных систем.
150. Основные функции подсистемы защиты операционных систем.