**Вопросы по предмету « Ethical hacking 2» на итоговый контроль**

1. Объясните разницу между “Gray hat hacking” и “black hat”.
2. Оцените законность деятельности хакеров “gray hat”, прокомментируйте свои мысли примерами.
3. Сравните “White hat hacking” и “gray hat hacking”.
4. В каких ситуациях может быть полезен “gray hat”?
5. Когда хакерство “gray hat” может быть этически приемлемым?
6. Какую роль играет “gray hat hacking” в обеспечении общественной безопасности?
7. При каких обстоятельствах “gray hat hacking” считается незаконным?
8. Какие юридические вопросы вызывает работа “gray hat” хакеров с крупными компаниями?
9. Проанализируйте плюсы и минусы “gray hat hacking” в кибербезопасности.
10. Напишите об этических нормах хакерства.
11. Объясните понятие “reverse engineering”.
12. Как используется “reverse engineering” в анализе программного обеспечения?
13. Объясните ключевые возможности инструмента Ghydra.
14. Объясните основные различия между "IDA Pro" и "Ghydra".
15. Анализируйте “reverse engineering” на законных основаниях.
16. Какую роль играют инструменты “reverse engineering” в кибербезопасности?
17. Опишите простой процесс анализа эксплоидов с помощью "Ghydra".
18. Опишите метод определения программного эксплойта с помощью "IDA Pro".
19. Как определить зашифрованную часть кода при “reverse engineering”?
20. Объясните связь между “reverse engineering” и эксплуататорским анализом.
21. С какими рисками сталкивается программист в процессе создания эксплойта?
22. В чем основные различия между эксплойтами Linux и эксплойтами Windows?
23. Какие методы используются для повышения эффективности эксплуатации?
24. Объясните основные ограничения безопасности, используемые в системе Linux.
25. Какие риски представляют собой эксплойты ядра “Windows kernel”?
26. Объясните анализ эксплойтов kernel.
27. Чем эксплойты PowerShell отличаются от других эксплойтов?
28. Объясните технологии, ограничивающие использование эксплойтов на уровне kernel.
29. Напишите об эффективных способах защиты от эксплойтов.
30. Как работает функция "ASLR (Address Space Layout Randomization)"?
31. Объясните основные различия между “Red Team” и “Purple Team”.
32. Каковы функции “Purple Team”?
33. Как атаки “Red Team” контролируются “Purple Team”?
34. Объясните трудности, с которыми пришлось столкнуться при организации деятельности “Purple Team”.
35. В чем преимущества совместной работы «Red Team» и «Purple Team»?
36. Роль “Red Team” в стратегии кибербезопасности.
37. Роль Фиолетовой команды в повышении безопасности организации.
38. Объясните основные этапы атаки “Red Team”.
39. Какие оборонительные стратегии использует “Blue Team”?
40. Какие инструменты играют важную роль в деятельности “Purple Team”?
41. Как работают “Command and Control”?
42. Какие угрозы несут в себе C2-системы?
43. Объясните методы идентификации и блокировки систем C2.
44. Какие инструменты используются для анализа C2-систем?
45. Какие существуют технологии для ограничения атак, связанных с C2-системами?
46. Объясните процесс работы сервера C2.
47. Напишите о влиянии систем C2 на социальное обеспечение.
48. Объясните современные техники C2-атак.
49. Напишите о принципе работы простой С2 атаки.
50. Анализируйте стратегии защиты систем C2.
51. Объясните основные этапы процесса “Threat Hunting”.
52. Как настроить лабораторию для “Threat Hunting”?
53. Прокомментируйте возможности инструментов “Threat Hunting”.
54. От чего зависит эффективность стратегии “Threat Hunting”?
55. Запишите проблемы, с которыми вы столкнетесь в лаборатории “Threat Hunting”.
56. Объясните процесс обнаружения угроз с помощью простого анализа “log”.
57. Какие инструменты эффективны при анализе угроз?
58. Какова роль «Threat Hunting» в кибербезопасности?
59. Какие алгоритмы используются для выявления угроз?
60. Объясните взаимосвязь между "Threat Hunting" и анализом эксплойтов.
61. Объясните основные технологии обнаружения эксплойтов Linux.
62. Какие существуют эффективные технологии защиты от эксплойтов Windows?
63. Объясните способы повышения безопасности на уровне ядра.
64. Оцените эффективность технологий защиты от эксплойтов.
65. Объясните преимущества и недостатки технологии "ASLR".
66. Как можно повысить безопасность при обнаружении эксплойтов?
67. Предлагайте новые технологии в области безопасности ядра.
68. Объясните основную сложность в обнаружении эксплойтов для Linux и Windows.
69. Каковы принципы безопасности операционной системы?
70. Как, по-вашему, будут развиваться современные исследователи?
71. Что такое эксплойты Linux и для каких целей они используются, на что делается основной упор при разработке этих эксплойтов?
72. Какие инструменты чаще всего используются для обнаружения и разработки эксплойтов ядра, какие возможности они предоставляют?
73. Перечислите основные инструменты, используемые для анализа уязвимостей в операционной системе Linux, и кратко прокомментируйте один из них.
74. Как работает эксплойт-инструмент “Metasploit Framework” и какую роль он играет в тестировании уязвимостей в системах Linux?
75. Вам было поручено найти уязвимый сервис, установленный в системе Linux, объяснить инструменты и шаги, которые вы используете в этом процессе.
76. Что такое переполнение буфера и к каким ошибкам оно может приводить?
77. Что такое “Pointers” и для чего они используются?
78. Объясните основное различие между сегментами "stack" и "heap" в языке программирования C.
79. Среди возможностей атаки — использование механизма для выявления слабых прав доступа к файлам и замены общей библиотеки вредоносной.
80. Какие технологии понадобятся для создания лаборатории по обнаружению угроз и каковы их основные требования?
81. В чем основные отличия между "DetectionLab" и "HELK" и в каком случае рекомендуется использовать каждый из них?
82. Какие факторы безопасности и стоимости следует учитывать при создании лаборатории обнаружения угроз в облаке?
83. Как правильно управлять и перезагружать лабораторию с помощью основных инструментов DetectionLab?
84. Какой вариант конфигурации "Docker Compose" следует выбрать при установке "HELK" и почему этот вариант подходит для лабораторных целей?
85. Нормализация источников данных с помощью OSSEM.
86. Визуализируйте источники данных с помощью OSSEM.
87. Что такое операции «стек»?
88. Каковы процедуры вызова функций?
89. Что такое переполнение буфера?
90. Как работают эксплойты локального переполнения буфера?
91. Как происходит процесс создания эксплойта?
92. Что такое метасплойт?
93. Возможности “PowerShell Empire”.
94. Что такое “Covenant”?
95. Принцип работы “Covenant”.
96. Возможности и применимость “Covenant”.
97. Что такое "декомпилятор" и "декомпиляция"?
98. “Ghidrada kod browser” и его функции.
99. Что такое “Gray hat”?
100. Слабые стороны "Bug Bounty" и их значение.
101. “Black hat hacking” — это черная шляпа.
102. Что такое «Cyber Kill Chain»?
103. Какие инструменты доступны для анализа карты памяти в IDA Pro?
104. Миссия и применение “Ghidra”.
105. Как искать и анализировать собственные функции в программе IDA Pro?
106. Объясните разницу между “Disassembly” и “Decompilation” в "IDA Pro".
107. Как анализировать данные “Strings” и “Imports” при использовании "IDA Pro"?
108. Какие инструменты доступны для анализа карты памяти в IDA Pro?
109. Подскажите рабочий процесс охоты на угрозы в сериале?
110. Расскажите нам о "MITRE ATT&CK Framework"