Теоретические задания муниципального этапа
всероссийской олимпиады школьников по технологии 2024-25 учебного года
профиль «Информационная безопасность»
10-11 класс

Общая часть

1. Что такое Brute Force?
1) технология, заключающаяся во внедрении в запрос к базе данных множественных обращений к информации и насильного отправления запросов к БД
2) технология «грубого» перебора паролей от учётных записей
3) технология взлома учётной записи, которая для своей работы обязательно требует список (базу данных) возможных паролей. Такие файлы иногда могут распространяться
4) технология социального инжиниринга, позволяющая получить у человека важную информацию, представляясь кем-то из его знакомых или родственников
5) технология социального инжиниринга, позволяющая получить у человека важную информацию, представляясь его начальником или подчиненным

2. Информационная безопасность обеспечивает…
1) блокирование информации
2) искажение информации
3) сохранность информации
4) утрату информации
5) подделку информации

3. Устройство для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающие маленький пейджер, не подсоединяемые к компьютеру и имеющие собственный источник питания:
1) токен
2) автономный токен
3) USB-токен
4) устройство iButton
5) смарт-карта

4. Аппаратные модули доверенной загрузки «Аккорд - АМДЗ» представляют собой…
1) аппаратный контролер
2) электронный замок
3) система контроля
4) сетевой адаптер
5) копировальный аппарат

5. Что такое кибербуллинг?
1) мошенничеств, совершаемое в сети Интернет
2) размещение в сети Интернет провокационных сообщений с целью вызвать конфликты между участниками беседы
3) любые сообщения или публикации в сети, размещаемые с целью запугать, оскорбить или иначе притеснить другого

Специальная часть

1. XSS – в компьютерной безопасности это
1) название SQL-инъекции для реализации уязвимости базы данных
2) принятая в странах Запада аббревиатура данных самого высокого уровня секретности
3) технология межсайтового выполнения сценариев, используемая для выполнения произвольного кода на веб-сервере во время взлома
4) технология внутрисайтового выполнения сценариев, используемая для выполнения произвольного кода на веб-сервере во время взлома

2. Основные принципы, на основании которых работают системы обнаружения вторжений (СОВ)
1) принцип недоказуемости вторжения
2) обнаружение на основании сигнатур
3) обнаружение на основании постоянного сканирования сетевых портов компьютера
4) обнаружение на основании аномалий

3. Выберите из предложенных вариантов пароля "правильный" (с точки зрения современных требований к паролю) (выберите один правильный вариант ответа):
1) 333998777
2) ГггКккОпр
3) 83466825710
4) Pfj-87H-Mt7

4. Вы обнаружили на рабочем столе своего ПК файл "Отчет_(Петров. И.Г)_2024.bat", вспомнили, что Петров И.Г. является сотрудником вашей компании. Это файл
1) отчет (вероятно, Петрова И.Г.) в виде документа
2) отчет (вероятно, Петрова И.Г.) в виде архива
3) файл с вирусом, вредоносной программой
4) файл с набором неизвестных команд

5. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:
1) авторизация
2) аутентификация
3) обезличивание
4) деперсонализация
5) идентификация

6. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:
1) авторизация
2) обезличивание
3) деперсонализация
4) аутентифика́ция
5) идентификация

7. Выберите наиболее точное определение понятия «Информационная безопасность»
1) набор программ, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения.

2) набор руководящих документов, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения.
3) набор процедур и инструментов, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения.

8. DLP-система в компьютерной безопасности это
1) система управления микрозеркалами матрицы в DLP-проекторах, применяемых для вывода изображений с высокой яркостью
2) система защиты от компьютерных атак извне крупной организации
3) специализированное ПО, предназначенное для защиты от утечек информации
4) специализированное ПО, предназначенное для борьбы с утечками персональных данных согласно ФЗ-152

9. CAPEC, CWE, CVE это
1) абревиатуры средств защиты информации и обеспечения контроля доступа в информационных системах
2) известные системы классификации уязвимостей
3) известные базы данных уязвимостей
4) программные инструменты для анализа уязвимостей

10. Как можно взломать данные, которые хранятся в цепочке Блокчейн, и можно ли это сделать в принципе
1) нет, это сделать невозможно, так как цепочка Блокчейн является основой построения криптовалюты Биткоин, скомпрометировать её нельзя
2) можно только расшифровать имеющуюся информацию, если применить методы потоковой криптографии
3) можно только расшифровать имеющуюся информацию, если применить методы квантовой криптографии
4) можно, для этого необходимо получить контроль над 50% компьютеров, входящих в систему +1 компьютер
5) это альтернативное название криптовалюты Биткоин

11. Эту функцию используют для контроля того, что файл не был изменен при хранении или передаче. Что это за функция (один ответ)
1) математическое преобразование, которое невозможно однозначно выполнить в обратную сторону
2) сумма четных бит информации для контроля четности
3) такое математическое преобразование, которое невозможно однозначно выполнить в прямом направлении и, в результате, хеш-сумма каждый раз будет разная
4) процесс проверки данных

12. IP-адрес DNS-сервера Yandex 77.88.8.8. Выберите, какой вариант вы укажете, если потребуется ввести данные в двоичном формате
1) 01001101.01011000.00001000.00001000
2) 01001011.01011010.00001000.00001000
3) 01001101.01011000.00100000.00100000
4) 01001101.01111000.00001000.00001000

13. Для передачи конфиденциальной информации по незащищенным каналом какую технологию используют

1) VPN
2) VPS
3) скремблирования
4) VDS
5) маскарадинга – «обертывания» IP-пакетов для работы с «серыми» IP-адресами

14. Были перехвачены двоичные данные, которые используются в качестве ключа для архива. Это два двоичных числа 101110101 и 1101101. Известно, что ключ является двоичной суммой этих чисел, а также – если ввести неправильную комбинацию, архив самоуничтожается. Какой ключ выберите для ондократной попытки открыть архив?
1) 111100100
2) 10110101
3) 1101101
4) 111100010
5) 101101101
6) 100001000
7) 011011101
8) 111101010

15. Закон 149-ФЗ это нормативный документ:
1. федерального уровня, регулирующий отношения и устанавливающий основные положения защиты персональных данных, собираемых, обрабатываемых и передаваемых в цифровом виде
2. федерального уровня, регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении ИТ и обеспечении защиты информации
3. закон о защите цифровой инфраструктуры от реализации основных угроз информационной безопасности – угрозы целостности, доступности, конфиденциальности информации.

Кейс-задание

Ваш сотрудник переслал на неизвестный электронный адрес письмо, был файл архива, закрытый паролем и текст. DLP-система заблокировала и отправила системному администратору. В письме был такой текст:

июъыьъэюърулплщфр
(допишешь в конец ROT№)

Системный администратор не смог подобрать пароль к архиву, помогите ему.