Финальный экзамен Результаты для Dmytro Zhurakovskyi

Оценка за эту попытку: **0** из 100
Отправлено 5 Май в 17:03
Эта попытка длилась 60 минут(ы).

Вопрос 1

0 / 2 балла (-ов)

Такие технологии, как IoE и GIS, способствуют накоплению огромных объемов данных. Назовите две причины, в силу которых эти технологии увеличивают спрос на специалистов по кибербезопасности. (Выберите два варианта.)

Ваш ответ — ☑ Требуется больше ресурсов для обработки данных.

то правильный ответ — В системах, созданных на основе этих технологий, хранятся персональные данные.

☐ Требуется больше оборудования.

Ваш ответ — ☑ Эти технологии усложняют структуру систем.

то правильный ответ — С помощью этих технологий ведется сбор конфиденциальной информации.

☐ Необходим круглосуточный мониторинг.

Refer to curriculum topic: 1.1.1
Растущая необходимость в надежной защите продиктована характером данных, собираемых с помощью этих технологий.

Нет ответа

Вопрос 2

0 / 2 балла (-ов)

Специалисту из отдела кадров предложили провести занятия с учащимися государственных школ, чтобы привлечь внимание молодых людей к сфере кибербезопасности. Назовите три темы, которым нужно уделить особое внимание на этих занятиях, чтобы мотивировать учащихся к построению карьеры в этой области? (Выберите три варианта.)

то правильный ответ ысокий доход

то правильный ответ ысокий спрос на специалистов

то правильный ответ лужение обществу

- должность, подразумевающая рутинную повседневную работу
- необходима докторская степень (PhD)
- сертификация CompTIA A+ обеспечивает достаточный уровень знаний для начала карьеры

Refer to curriculum topic: 1.2.2
Высокий спрос на специалистов по кибербезопасности открывает уникальные карьерные возможности.

Нет ответа

Вопрос 3

0 / 2 балла (-ов)

Назовите категорию, к которой относятся киберпреступники, создающие вредоносное ПО для компрометации компаний посредством кражи данных кредитных карт?

- «серые» хакеры

то правильный ответ «черные» хакеры

- «белые» хакеры
- хакеры-дилетанты

Refer to curriculum topic: 1.2.1
Хакеры определенных категорий похищают информацию с помощью вредоносного ПО.

Нет ответа

Вопрос 4

0 / 2 балла (-ов)

В каких трех состояниях данные уязвимы для атак? (Выберите три варианта.)

то правильный ответ — хранимые данные

- [ ] удаленные данные

то правильный ответ — обрабатываемые данные

- [ ] зашифрованные данные
- [ ] расшифрованные данные

то правильный ответ — передаваемые данные

Refer to curriculum topic: 2.3.1
Чтобы обеспечить эффективную защиту данных, специалист по кибербезопасности должен понимать суть каждого из трех ключевых состояний. Удаленные данные ранее находились в состоянии хранения. Зашифрованные и расшифрованные данные могут находиться в любом из трех ключевых состояний.

Нет ответа

Вопрос 5

0 / 2 балла (-ов)

Назовите технологию, с помощью которой можно было бы в принудительном порядке обеспечить соблюдение политики безопасности, согласно которой вычислительное устройство может быть

подключено к сети комплекса зданий лишь при условии, что на этом устройстве установлено последнее обновление антивирусного ПО.

- NAS
- VPN
- сеть хранения данных (SAN)

то правильный ответ NAC

Refer to curriculum topic: 2.4.1
Специалист по кибербезопасности должен быть хорошо знаком с современными технологиями, позволяющими усилить политику безопасности, действующую в его организации.

Нет ответа

Вопрос 6

0 / 2 балла (-ов)

Назовите методы, с помощью которых можно внедрить многофакторную аутентификацию.

то правильный ответ пароли и отпечатки пальцев

- системы IDS и IPS
- токены и хеш-суммы
- сети VPN и VLAN

Refer to curriculum topic: 2.2.1
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии для поддержки триады «конфиденциальность, целостность, доступность».

Нет ответа

Вопрос 7

0 / 2 балла (-ов)

Какую технологию идентификации можно использовать в составе системы аутентификации сотрудников?

- виртуальный отпечаток пальца
- Хеширование SHA-1

то правильный ответ

- считывание смарт-карт
- тамбур-шлюз

Refer to curriculum topic: 2.2.1
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии для поддержки триады «конфиденциальность, целостность, доступность».

Нет ответа

Вопрос 8

0 / 2 балла (-ов)

Специалист по кибербезопасности совместно с сотрудниками подразделения ИТ работает над планом информационной безопасности. Какой набор принципов безопасности следует взять за основу при разработке плана информационной безопасности?

- секретность, идентификация, невозможность отказа

то правильный ответ

- конфиденциальность, целостность, доступность
- шифрование, аутентификация, идентификация
- технологии, политики, осведомленность

Refer to curriculum topic: 2.1.1
Конфиденциальность, целостность и доступность берутся за основу при разработке всех систем управления.

Нет ответа

Вопрос 9

0 / 2 балла (-ов)

К какому типу относится атака, при которой мошеннические веб-сайты размещаются на высоких позициях в списках результатов веб-поиска?

- атака путем подделки DNS
- угонщик браузеров

то правильный ответ

- злоупотребление поисковой оптимизацией
- спам

Refer to curriculum topic: 3.1.2
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Нет ответа

Вопрос 10

0 / 2 балла (-ов)

Назовите три лучших способа для защиты от атак с использованием социальной инженерии. (Выберите три варианта.)

то правильный ответ

- Не переходить по ссылкам, вызывающим любопытство.

то правильный ответ

- Повысить осведомленность сотрудников относительно действующих политик.
- Внедрить эффективные межсетевые экраны.

то правильный ответ

- Не вводить пароли в окне чата.
- Внедрить политику, согласно которой сотрудники ИТ-подразделения имеют право передавать информацию по телефону только руководителям.

Увеличить число охранников.

Refer to curriculum topic: 3.2.2
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии и средства, которые используются в качестве контрмер для защиты организации от угроз и нейтрализации уязвимостей.

Нет ответа

Вопрос 11

0 / 2 балла (-ов)

Назовите нетехнический метод, с помощью которого киберпреступники получают конфиденциальную информацию.

- фарминг
- атака через посредника

то правильный ответ

- социальная инженерия
- программа-вымогатель

Refer to curriculum topic: 3.2.1
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Нет ответа

Вопрос 12

0 / 2 балла (-ов)

Сотрудники компании получают электронные письма, в которых говорится, что срок действия пароля учетной записи истекает в ближайшее время и поэтому нужно сменить пароль в течение 5 минут. Какое из описаний подходит для такого электронного сообщения?

то правильный ответ Обман.

Атака, при которой злоумышленник выдает себя за авторизованную сторону.

Атака, при которой злоумышленник проникает в систему, пользуясь действующим подключением авторизованного пользователя.

DDoS-атака.

Refer to curriculum topic: 3.2.2
Методы социальной инженерии включают несколько различных тактик для получения информации от жертв.

Нет ответа

Вопрос 13

0 / 2 балла (-ов)

К какому типу относится атака, при которой сотрудник подключает к сети организации неавторизованное устройство для отслеживания сетевого трафика?

рассылка спама

то правильный ответ прослушивание

фишинг

подмена

Refer to curriculum topic: 3.3.1
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Нет ответа

Вопрос 14

0 / 2 балла (-ов)

Назовите два наиболее эффективных метода защиты от вредоносного ПО. (Выберите два варианта.)

- [ ] Применение RAID.
- [ ] Внедрение сети VPN.

то правильный ответ

Своевременное обновление операционной системы и остального программного обеспечения.

- [ ] Внедрение межсетевых экранов.
- [ ] Применение надежных паролей.

то правильный ответ

Установка и своевременное обновление антивирусного ПО.

Refer to curriculum topic: 3.1.1
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии и средства, которые используются в качестве контрмер для защиты организации от угроз и нейтрализации уязвимостей.

Нет ответа

Вопрос 15

0 / 2 балла (-ов)

В компании организовали проверку защищенности сети путем тестирования на проникновение. Проверка показала, что в сети присутствует бэкдор. Какие меры следует принять в этой организации, чтобы выяснить, скомпрометирована ли сеть?

то правильный ответ

Проверить системы на наличие неавторизованных учетных записей.

- [ ] Проверить, нет ли учетных записей без паролей.
- [ ] Проверить системы на наличие вирусов.

Проверить в журнале событий, не было ли изменений в политике.

Refer to curriculum topic: 3.1.1
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Нет ответа

Вопрос 16

0 / 2 балла (-ов)

Какое из утверждений относится к блочным шифрам?

Алгоритмы блочного шифрования быстрее алгоритмов поточного шифрования.

Блочное шифрование сжимают шифруемую информацию.

то правильный ответ

При блочном шифровании объем зашифрованных данных обычно больше объема исходных данных.

Алгоритмы блочного шифрования обрабатывают открытый текст по одному биту и формируют из битов блоки.

Refer to curriculum topic: 4.1.2
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Нет ответа

Вопрос 17

0 / 2 балла (-ов)

Как называется механизм безопасности, к которому относятся пароли, парольные фразы и PIN-коды?

то правильный ответ

- аутентификация
- авторизация
- доступ
- идентификация

Refer to curriculum topic: 4.2.4
Для усиления систем контроля доступа применяются различные методы аутентификации. Нужно понимать особенности каждого из этих методов.

Нет ответа

Вопрос 18

0 / 2 балла (-ов)

Какой алгоритм применяется в Windows по умолчанию при шифровании файлов и папок на томе NTFS?

- RSA
- DES
- 3DES

то правильный ответ

- AES

Refer to curriculum topic: 4.1.4
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Нет ответа

Вопрос 19

0 / 2 балла (-ов)

Какой метод применяется в стеганографии для сокрытия текста внутри файла изображения?

- маскирование данных
- обфускация данных
- изменение старшего бита

то правильный ответ изменение младшего бита

Refer to curriculum topic: 4.3.2
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Нет ответа

Вопрос 20

0 / 2 балла (-ов)

К какому типу средств контроля доступа относятся смарт-карты и системы биометрической идентификации?

- физические
- технологические

то правильный ответ логические

- административные

Refer to curriculum topic: 4.2.1
Контроль доступа препятствует получению доступа неавторизованным пользователем к конфиденциальным данным и сетевым системам. Существует несколько технологий, с помощью которых реализуются эффективные стратегии контроля доступа.

Нет ответа

Вопрос 21

0 / 2 балла (-ов)

Алиса и Боб обмениваются конфиденциальными сообщениями, пользуясь общим PSK-ключом. Если Боб пожелает отправить сообщение Кэрол, то каким ключом нужно будет зашифровать это сообщение?

то правильный ответ

новый общий PSK-ключ

- открытый ключ Боба
- общий PSK-ключ, которым шифруются сообщения, адресованные Алисе
- закрытый ключ Кэрол

Refer to curriculum topic: 4.1.2
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Нет ответа

Вопрос 22

0 / 2 балла (-ов)

Какие средства контроля доступа должны будут применить сотрудники подразделения ИТ, чтобы восстановить нормальное состояние системы?

компенсирующие

то правильный ответ корректирующие

превентивные

распознавательные

Refer to curriculum topic: 4.2.7
Контроль доступа препятствует получению доступа неавторизованным пользователем к конфиденциальным данным и сетевым системам. Существует несколько технологий, с помощью которых реализуются эффективные стратегии контроля доступа.

Нет ответа

Вопрос 23

0 / 2 балла (-ов)

В организации внедрили антивирусное ПО. К какому типу относится это средство контроля безопасности?

компенсационные средства контроля

сдерживающие средства контроля

средства обнаружения

то правильный ответ средства восстановления

Refer to curriculum topic: 4.2.7
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии и средства, которые используются в качестве контрмер для защиты организации от угроз и нейтрализации уязвимостей.

Нет ответа

Вопрос 24

0 / 2 балла (-ов)

Какую технологию следует внедрить, чтобы иметь возможность идентифицировать организацию, выполнить аутентификацию веб-сайта этой организации и установить зашифрованное соединение между клиентом и веб-сайтом?

- асимметричное шифрование
- добавление соли
- цифровая подпись

то правильный ответ цифровой сертификат

Refer to curriculum topic: 5.2.2
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Нет ответа

Вопрос 25

0 / 2 балла (-ов)

Какой алгоритм хеширования следует использовать для защиты конфиденциальной несекретной информации?

- AES-256
- MD5
- 3DES

то правильный ответ SHA-256

Refer to curriculum topic: 5.1.1
Целостность данных является одним из трех руководящих принципов обеспечения информационной безопасности. Специалист по обеспечению кибербезопасности должен быть знаком со средствами и технологиями, предназначенными для обеспечения целостности данных.

Нет ответа

Вопрос 26

0 / 2 балла (-ов)

Какая технология хеширования подразумевает обмен ключами?

- MD5
- добавление соли
- AES

то правильный ответ HMAC

Refer to curriculum topic: 5.1.3
Механизм HMAC отличается от обычного хеширования наличием ключей.

Нет ответа

Вопрос 27

0 / 2 балла (-ов)

Вам поручили провести работу с сотрудниками, отвечающими за сбор и ввод данных в вашей организации: нужно улучшить контроль целостности данных при вводе и модификации. Некоторые сотрудники просят объяснить, с какой целью в новых формах для ввода данных введены ограничения по типу и длине вводимых значений. Что из перечисленного можно назвать новым средством контроля целостности данных?

средства контроля ввода, допускающие лишь просмотр текущих данных

шифрование данных, благодаря которому доступ к конфиденциальным данным имеют только авторизованные пользователи

ограничение, согласно которому ввод конфиденциальных данных могут выполнять только авторизованные сотрудники

то правильный ответ

правило проверки ввода, гарантирующее полноту, точность и непротиворечивость данных

Refer to curriculum topic: 5.4.2
Целостность данных обеспечивается путем их проверки.

Нет ответа

Вопрос 28

0 / 2 балла (-ов)

Назовите главную особенность криптографической хеш-функции.

Выходные значения имеют различную длину.

По выходному значению хеш-функции можно вычислить входное значение.

Для хеширования необходимы открытый и закрытый ключи.

то правильный ответ

Хеш-функция необратима.

Refer to curriculum topic: 5.1.1
Целостность данных является одним из трех руководящих принципов обеспечения информационной безопасности. Специалист по обеспечению кибербезопасности должен быть знаком со средствами и технологиями, предназначенными для обеспечения целостности данных.

Нет ответа

Вопрос 29

0 / 2 балла (-ов)

Назовите метод, с помощью которого можно сгенерировать разные хеш-суммы для одинаковых паролей.

- HMAC
- SHA-256

то правильный ответ

- добавление соли
- CRC

Refer to curriculum topic: 5.1.2
Целостность данных является одним из трех руководящих принципов обеспечения информационной безопасности. Специалист по кибербезопасности должен быть знаком со средствами и технологиями обеспечения целостности данных.

Нет ответа

Вопрос 30

0 / 2 балла (-ов)

Вам поручили разъяснить суть механизма проверки данных сотрудникам отдела дебиторской задолженности, выполняющим ввод данных. Выберите наилучший пример для иллюстрации типов данных «строка», «целое число», «десятичная дробь».

- 800-900-4560, 4040-2020-8978-0090, 21.01.2013

да/нет 345-60-8745, TRF562

мужчина, 25,25 $, ветеран

то правильный ответ женщина, 9866, 125,50 $

Refer to curriculum topic: 5.4.2
Строка — это набор букв, цифр и специальных символов. Целое число — это число без дробной части. Десятичная дробь — это дробное число в десятичной форме.

Нет ответа

Вопрос 31

0 / 2 балла (-ов)

Назовите технологию, с помощью которой можно предотвратить атаку, реализуемую методом перебора по словарю или методом грубой силы с использованием хеш-суммы?

то правильный ответ HMAC

AES

MD5

радужные таблицы

Refer to curriculum topic: 5.1.3
В HMAC используется дополнительный секретный ключ, который принимает хэш-функция. Таким образом, помимо хеширования, присутствует дополнительный уровень безопасности, что позволяет нейтрализовать атаку через посредника (MitM) и обеспечить аутентификацию источника данных.

Нет ответа

Вопрос 32

0 / 2 балла (-ов)

К какому типу стратегий снижения рисков относятся такие меры, как приобретение страховки и привлечение сторонних поставщиков услуг?

- снижение риска
- уклонение от риска
- принятие риска

то правильный ответ передача риска

Refer to curriculum topic: 6.2.1
Меры по снижению рисков уменьшают степень уязвимости организации к угрозам, что достигается за счет передачи, принятия или снижения риска, а также уклонения от него.

Нет ответа

Вопрос 33

0 / 2 балла (-ов)

Какие две величины необходимы для расчета ожидаемого годового объема убытков? (Выберите два варианта.)

- ценность ресурса
- мера уязвимости ресурса к угрозе

то правильный ответ ожидаемый ущерб в результате реализации единичной угрозы

то правильный ответ количество реализаций угрозы в год

- количественная величина убытков
- коэффициент частоты

Refer to curriculum topic: 6.2.1
При количественном анализе рисков используются следующие величины: ожидаемый ущерб в результате реализации единичной угрозы; количество реализаций угрозы в годовом исчислении; ожидаемый объем убытков в годовом исчислении.

Нет ответа

Вопрос 34

0 / 2 балла (-ов)

В организации устанавливают только те приложения, которые соответствуют внутренним нормам. Все остальные приложения удаляются администраторами в целях усиления безопасности. Как называется этот метод?

- классификация ресурсов
- идентификация ресурсов

то правильный ответ

- стандартизация ресурсов
- доступность ресурсов

Refer to curriculum topic: 6.2.1
Организации необходимо знать, какое аппаратное обеспечение и какие программы имеются в наличии, чтобы знать, какими должны быть параметры конфигурации. Управление ресурсами охватывает все имеющееся аппаратное и программное обеспечение. В стандартах ресурсов определены все отдельные продукты аппаратного и программного обеспечения, которые использует и поддерживает организация. В случае сбоя оперативные действия помогут сохранить доступность и безопасность.

Нет ответа

Вопрос 35

0 / 2 балла (-ов)

Группа специалистов проводит анализ рисков применительно к сервисам БД. Помимо прочего, специалисты собирают следующую информацию: первоначальная ценность ресурсов; существующие угрозы для этих ресурсов; ущерб, который могут нанести эти угрозы. На основании собранной информации специалисты рассчитывают ожидаемый годовой объем убытков. Какой вид анализа рисков выполняет группа?

то правильный ответ

- количественный анализ
- анализ потерь
- качественный анализ
- анализ защищенности

Refer to curriculum topic: 6.2.1
Качественный или количественный анализ рисков используется для определения угроз организации и распределения их по приоритетам.

Нет ответа

Вопрос 36

0 / 2 балла (-ов)

Риск-менеджер вашей организации представил схему, где уровни угрозы для ключевых ресурсов систем информационной безопасности обозначены тремя цветами. Красный, желтый и зеленый цвета обозначают соответственно высокий, средний и низкий уровень угрозы. Какому виду анализа рисков соответствует такая схема?

- количественный анализ
- анализ степени уязвимости к угрозам

то правильный ответ

- качественный анализ
- анализ потерь

Refer to curriculum topic: 6.2.1
Качественный или количественный анализ рисков используется для определения угроз организации и распределения их по приоритетам.

Нет ответа

Вопрос 37

0 / 2 балла (-ов)

Назовите подход к обеспечению доступности, при котором используются разрешения на доступ к файлам?

- упрощение
- то правильный ответ ограничение
- многоуровневый подход
- сокрытие информации

Refer to curriculum topic: 6.2.2
Обеспечение доступности систем и данных составляет особо важную обязанность специалиста по кибербезопасности. Важно понимать технологии, процессы и средства контроля, с помощью которых обеспечивается высокая доступность.

Нет ответа

Вопрос 38

0 / 2 балла (-ов)

Назовите два этапа реагирования на инциденты. (Выберите два варианта.)

- конфиденциальность и ликвидация
- то правильный ответ изоляция и восстановление
- анализ рисков и высокая доступность

- устранение угроз и принятие

то правильный ответ - обнаружение и анализ

- предотвращение и изоляция

Refer to curriculum topic: 6.3.1
Организация должна знать, как реагировать на произошедший инцидент. Необходимо разработать и применять план реагирования на инциденты, включающий несколько этапов.

Нет ответа

Вопрос 39

0 / 2 балла (-ов)

Какому из принципов высокой доступности соответствует формулировка «сохранение доступности в аварийных ситуациях»?

- единая точка отказа
- отказоустойчивость
- бесперебойное обслуживание

то правильный ответ - отказоустойчивость системы

Refer to curriculum topic: 6.1.1
Высокая доступность достигается следующими методами: полное или частичное исключение ситуаций, при которых отказ единичного компонента влечет за собой отказ всей системы; повышение отказоустойчивости системы в целом; проектирование системы с учетом требований к отказоустойчивости.

Нет ответа

Вопрос 40

0 / 2 балла (-ов)

К какой категории методов аварийного восстановления относится размещение резервных копий на удаленной площадке?

- корректирующие
- распознавательные
- то правильный ответ превентивные
- административные

Refer to curriculum topic: 6.4.1
План аварийного восстановления помогает подготовить организацию к потенциальным аварийным ситуациям и минимизировать время простоя.

Нет ответа

Вопрос 41

0 / 2 балла (-ов)

Назовите три протокола, допускающие использование симметричного алгоритма блочного шифрования (AES). (Выберите три варианта.)

- то правильный ответ 802.11i
- то правильный ответ WPA
- 802.11q
- то правильный ответ WPA2
- TKIP
- WEP

Refer to curriculum topic: 7.3.1
Защищенную систему связи можно организовать с помощью различных протоколов. Алгоритм AES является наиболее стойким алгоритмом шифрования.

Нет ответа

Вопрос 42

0 / 2 балла (-ов)

Какую технологию можно использовать для защиты от несанкционированного прослушивания голосового трафика, передаваемого с помощью VoIP-соединений?

- SSH
- ARP
- сильная аутентификация

то правильный ответ — шифрование голосового трафика

Refer to curriculum topic: 7.3.2
Многие передовые технологии, включая VoIP, передачу потокового видео и конференц-связь, требуют соответствующих мер безопасности.

Нет ответа

Вопрос 43

0 / 2 балла (-ов)

Какое из перечисленных утверждений точнее всего соответствует забору высотой в 1 метр?

- Забор ограждает территорию от случайных прохожих благодаря своей высоте.

Забор сможет противостоять нарушителю, намеренно проникающему на территорию.

Забор ненадолго задержит нарушителя, намеренно проникающего на территорию.

то правильный ответ Забор сдерживает только случайных прохожих.

Refer to curriculum topic: 7.4.1
Существуют стандарты безопасности, помогающие внедрить адекватные средства контроля доступа в организациях для устранения потенциальных угроз. Эффективность защиты территории от проникновения посторонних определяется высотой забора.

Нет ответа

Вопрос 44

0 / 2 балла (-ов)

Что означает термин «точка баланса вероятностей ошибок», если речь идет о сравнении биометрических систем?

степень неприемлемости и количество ложноотрицательных срабатываний

количество ложноположительных срабатываний и степень приемлемости

степень приемлемости и количество ложноотрицательных срабатываний

то правильный ответ количество ложноотрицательных результатов и количество ложноположительных результатов

Refer to curriculum topic: 7.4.1
При сравнении биометрических систем следует учитывать ряд важных факторов, включая точность, скорость (пропускную способность) и степень приемлемости для пользователей.

Нет ответа

Вопрос 45

0 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

- DNS
- то правильный ответ ping
- RIP
- NTP

Refer to curriculum topic: 7.3.1
С помощью протокола ICMP сетевые устройства передают сообщения об ошибках.

Нет ответа

Вопрос 46

0 / 2 балла (-ов)

Какие атаки можно предотвратить с помощью взаимной аутентификации?

- беспроводной спам
- анализ беспроводного трафика
- то правильный ответ атака через посредника
- подмена IP-адреса отправителя в беспроводных сетях

Refer to curriculum topic: 7.1.2
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии и средства, которые используются в качестве контрмер для защиты организации от угроз и нейтрализации уязвимостей.

Нет ответа

Вопрос 47

0 / 2 балла (-ов)

Какой из перечисленных инструментов лучше подходит для создания снимка базового состояния операционной системы?

- CVE Baseline Analyzer
- SANS Baselining System (SBS)
- MS Baseliner

то правильный ответ Microsoft Security Baseline Analyzer

Refer to curriculum topic: 7.1.1
Существует множество инструментов, с помощью которых специалист по кибербезопасности оценивает потенциальные уязвимости организации.

Нет ответа

Вопрос 48

0 / 2 балла (-ов)

Почему для тестирования безопасности сети организации часто выбирают дистрибутив Kali Linux?

- Это инструмент сканирования сети, который определяет приоритеты для угроз безопасности.

Он может использоваться для перехвата и регистрации сетевого трафика.

то правильный ответ

Это дистрибутив Linux с открытым исходным кодом, включающий в себя более 300 инструментов для защиты.

Он может использоваться для проверки слабых мест только с помощью вредоносного ПО.

Refer to curriculum topic: 8.2.4
Kali — это дистрибутив Linux с открытым исходным кодом, используемый многими ИТ-специалистами для тестирования безопасности сетей.

Нет ответа

Вопрос 49

0 / 2 балла (-ов)

Какие три услуги предоставляют CERT? (Выберите три варианта.)

то правильный ответ

Разработка инструментов, продуктов и методик технической экспертизы

то правильный ответ

Устранения уязвимостей программного обеспечения

Разработка инструментов атаки

то правильный ответ

Разработка инструментов, продуктов и методик для анализа уязвимостей

Соблюдение стандартов программного обеспечения

Создание инструментов для разработки вредоносного ПО

Refer to curriculum topic: 8.2.3
Услуги CERT включают:

- помощь в устранении уязвимостей ПО;
- разработку инструментов, продуктов и методик для технической экспертизы;
- разработку инструментов, продуктов и методик для анализа уязвимостей;
- разработку инструментов, продуктов и методик для мониторинга крупных сетей;
- помощь организациям в оценке эффективности методов, используемых ими для обеспечения безопасности.

Нет ответа

Вопрос 50

0 / 2 балла (-ов)

Какие три исключения из правил по обязательному предоставлению информации предусмотрены Законом о свободе информации (FOIA)? (Выберите три варианта.)

то правильный ответ

Документация правоохранительных органов, попадающая под перечисленные исключения

Общедоступная информация финансовых учреждений

Негеологическая информация о скважинах

то правильный ответ

Конфиденциальная коммерческая информация

то правильный ответ

Информация, касающаяся национальной безопасности и внешней политики

Информация, не защищенная специальными законами

Refer to curriculum topic: 8.2.2
Закон о свободе информации (FOIA) предусматривает следующие исключения:

1. Информация, касающаяся национальной безопасности и внешней политики
2. Внутренние правила и практики для сотрудников государственных органов
3. Информация, защищенная специальными законами
4. Конфиденциальная коммерческая информация
5. Сведения, передаваемые внутри органов или между ними и попадающие под адвокатскую тайну (в связи с совещательными процессами, судебными разбирательствами и т. д.)
6. Информация, которая в случае раскрытия может расцениваться как явное незаконное вторжение в личную жизнь
7. Документация правоохранительных органов, попадающая под перечисленные исключения
8. Данные государственных органов, полученные от финансовых учреждений
9. Геологическая и геофизическая информация о скважинах

Оценка контрольной работы: **0** из 100