Всероссийская олимпиада школьников по технологии школьный этап

10-11 класс

«Информационная безопасность»

2024– 2025 учебный год

*Специальная часть*

*Задание 1.*

Наиболее универсальным подходом к повышению защиты от угроз информационной безопасности является

|  |  |
| --- | --- |
|  | Непрерывный мониторинг и анализ сетевой активности |
|  | Ограничение доступа ко всем сетям, включая локальные |
|  | Регулярное обновление архитектуры и конфигураций защищаемой системы с целью усложнить исследование системы злоумышленником и разработку инструментов для осуществления атак |
|  | **Обучение пользователей основам кибербезопасности и осведомленности о рисках** |
|  | Развёртывание в защищаемой системе максимально возможного набора средств защиты различной направленности – сетевой, антивирусной, криптографической и т. д. |

**За верный ответ – 1 балл.**

*Задание 2.*

Сопоставьте категории вредоносного программного обеспечения с их характерными особенностями.

|  |  |  |
| --- | --- | --- |
| 1. Сетевой червь |  | **А.** Внедряет рекламу в системы, часто без согласия пользователя |
| 2. Бэкдор |  | **Б.** Маскируется под легальную программу |
| 3. Спуфер |  | **В.** Позволяет обойти штатные средства защиты |
| 4. Троянская программа |  | **Г.** Может создавать свои копии |
| 5. Адваре |  | **Д.** Предназначены для подделки информации |

Ответ; 1Г, 2В, 3Д, 4 Б, 5А

**За верный ответ – 1 балл.**

**Максимум за задание 5 баллов.**

*Задание 3.*

Какой из этих методов НЕ является безопасным для хранения паролей?

|  |  |
| --- | --- |
|  | Использовать длинные и сложные пароли |
|  | **Хранить пароли в текстовых файлах на компьютере** |
|  | Изменять пароли регулярно |
|  | Использовать менеджеры паролей |
|  | Не использовать один и тот же пароль для разных учетных записей |

**За верный ответ – 1 балл.**

*Задание 4.*

Вся история развития ЭТОЙ индустрии включает в себя очень много занимательных страниц, однако о самой первой из этих страниц до сих пор ведутся нескончаемые споры. Кто же всетаки придумал ИХ? Когда же появилась самая первая ОНА? Различные источники ссылаются на совершенно различную информацию на этот счет.

Есть такое мнение, что самую первую ЕЁ разработал еще в 1984 году американский программист Энди Хопкинс. Первая ОНА в современном понимании этого термина появилась в 1985 году усилиям Джи Вонга.

Ну, а на отечественном рынке нашим истинным первопроходцем стал Дмитрий Николаевич Лозинский, который разработал ЕЁ в 1988 году, практически одновременно с Макафи.

О чем идет речь в тексте, назовите ЕЁ двумя словами.

Ответ: Антивирусная программа

**За верный ответ – 3 балла.**

*Задание 5.*

Дан список утверждений. Оцените, является ли верным каждое из них

|  |  |  |
| --- | --- | --- |
| Цифровые водяные знаки – это структуры данных, встраиваемые в цифровые объекты (например, файлы), на основе методов стеганографии | **Верно** | Неверно |
| В ассиметричном шифровании задействован один и тот же криптографический ключ | Верно | **Неверно** |
| При вводе логина пользователь предоставляет информацию для авторизации | Верно | **Неверно** |
| Для запуска троянской программы, не обладающей другими возможностями, обычно требуется запуск пользователем программы, содержащей вредоносные функции | **Верно** | Неверно |
| Политика безопасности в системе (сети) – это комплекс руководств, требований обеспечения необходимого уровня безопасности | **Верно** | Неверно |

**За верный ответ – 1 балл.**

**Максимум за задание 5 баллов.**

*Задание 6.*

Выбрать ВСЕ верные продолжения фразы.

Недавно созданные, ещё не изученные вредоносные программы…

|  |  |
| --- | --- |
|  | можно обнаружить при помощи сигнатур |
|  | невозможно обнаружить антивирусными средствами |
|  | **можно обнаружить при помощи анализа кода программы** |
|  | **можно обнаружить при помощи анализа перечня запущенных в системе процессов** |

**За верный ответ – 2 балла.**

*Задание 7.*

Укажите, что не может являться адресом сайта

|  |  |
| --- | --- |
|  | sodgmsdkaojgij.ru |
|  | **besttravel** |
|  | 206.188.192.188 |
|  | ru. myshop.info |

**За верный ответ – 2 балла.**

*Задание 8.*

Какой протокол используется для защищенной передачи данных в интернете?

|  |  |
| --- | --- |
|  | FTP |
|  | SMTP |
|  | **HTTPS** |
|  | POP3 |
|  | HTTP |

**За верный ответ – 1 балл.**

*Задание 9.*

К какому типу атаки на пароль относится перебор всех комбинаций допустимых символов (начиная от односимвольных паролей)?

|  |  |
| --- | --- |
|  | Досс-атака |
|  | **Грубой силы** |
|  | Сниффинг |
|  | Фишинг |
|  | Интерсепция |

**За верный ответ – 2 балла.**

*Задание 10.*

Протоколом передaчи фaйлов по сети, появившийся в 1971 году нaзывeтся?

|  |  |
| --- | --- |
|  | DNS |
|  | HTTP |
|  | DHCP |
|  | **FTP** |
|  | Proxy |

**За верный ответ – 2 балла.**

*Задание 11.*

***Справочная информация***

*«Решетка Кардано» — это первая известная в истории шифровальная решетка, являющаяся трафаретом, который использовался для шифрования и дешифрования. Название данного шифра происходит от имени его создателя, известного итальянского ученого Джероламо Кардано.*

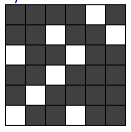
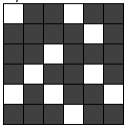
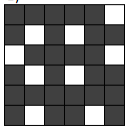
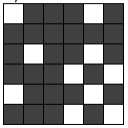
*Основой самой простой решетки Кардано является трафарет, исполненный в виде квадратной таблицы n × n клеток, некоторые из которых вырезаны (в том числе, возможно, и имеющие общую сторону или вершину). Клетки должны иметь такой размер, чтобы в каждую помещалась ровно одна буква. Вырезанные клетки должны располагаться таким образом, чтобы никакие две из них не оказывались в одном и том же месте при поворотах решётки.*

*Чтобы зашифровать сообщение, нужно разместить решётку на бумаге и вписать часть текста в вырезанные клетки, затем повернуть решётку на 90° и вписать следующую часть и т. д. После этого в оставшиеся пустыми места на бумаге нужно вписать произвольные символы (разумеется, для лучшей маскировки нужно использовать символы из того же алфавита, что и символы, из которых состоит сообщение).*

*Решётка Кардано в своём первоначальном виде более является источником литературного, нежели криптографического интереса. Например, рукопись Войнича, которая могла быть поддельной шифровкой XVI века, возможно, была построена с помощью решётки Кардано, примененной для того, чтобы составить псевдослучайную бессмыслицу из ранее существовавшего текста.*

Из четырех возможных решётки –ключа, выберите ту, которая является корректным ключом описанного шифра.

А) Б) В) Г)



Ответ: Б

**За верный ответ – 7 баллов.**

*Задание 12.*

Текст зашифрованный с помощью Решетка Кардано:

АМНСИСНФВААЬВКАСЕОИЕМТРОНЛШЦЫЛФРИЯРЬЕВМВЗИЕХЯАКТ

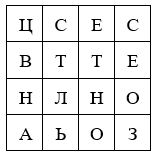
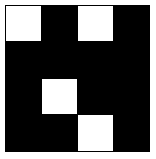
Установите, может ли в нём быть слово «трансформация»

Ответ: ДА

**За верный ответ – 3 балла.**

*Задание 13.*

Шифротекст, полученный с использованием решётки Кардано. Расшифруйте текст

Ответ: Целостность звена

**За верный ответ – 5 баллов.**

*Задание 14.*

Установите соответствие между методом шифрования и его описанием:

|  |  |  |
| --- | --- | --- |
| 1.Шифрование методом подстановки |  | А. Шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор |
| 2. Шифрование методом аналитических преобразований |  | Б. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности |
| 3. Шифрование методом перестановки |  | В. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов |
| 4. Шифрование методом гаммирования |  | Г. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста |

Ответ: 1В, 2А, 3Г,4Б

**За верный ответ – 1 балл.**

**Максимум за задание 4 балла.**

*Задание 15.*

Какой из следующих методов обеспечивает целостность данных?

|  |  |
| --- | --- |
|  | Шифрование |
|  | **Хеширование** |
|  | Кодирование |
|  | Декодирование |
|  | Сжатие |

**За верный ответ – 2 балла.**

**Кейс задание**

В начале года делегация ученых университета N отправился на конференцию в далекие страны. Материал, который планировали презентовать и обсудить по-современному с использованием планшетов Xiaomi, был утерян. Оказалось, что смартфоны и планшеты всей делегации университета N не содержат докладов и файлов, подготовленных для выступления.

Вскоре началось расследование инцидента. У всех сразу аккаунты взломать не могли, и служба безопасности заподозрила, что угроза исходит из корпоративной сети. Сервер с базой данных, где хранятся пароли, был с подозрительно старой версией Munin – системой мониторинга статусов сервисов сети. Старые версии Munin отличаются большим количеством незакрытых уязвимостей. После проверки оказалось, что злоумышленник воспользовался одной из таких уязвимостей старой версии, SQL-инъекцией, и выдал себе права администратора, получив таким образом доступ к базе данных Munin. Специалист по расследованию инцидентов также обнаружил, что в оперативной памяти одного из контроллеров домена корпоративной сети обнаружились явные признаки компрометации, а исходящие сетевые соединения были осуществлены на IP-адрес частного хостинга, находящегося в государстве Т.

К тому же неизвестный процесс запущен с PPID (идентификатор процесса), не отображающимся в списке процессов. При проверке процесса на наличие вирусов, оказалось, что тело процесса имело типичные для вредоносного ПО изменения. Файл имел небольшой вес, считывал нажимаемые клавиши, создавал логи в зашифрованном виде и отправлял их по сети посредством HTTPS. Кроме того, в ходе расследования выяснилось, что несмотря на то, что базы данных Munin и контроллера домена корпоративной сети различны, администратор Munin и по совместительству администратор контроллера домена использовал одинаковые логин и пароль для входа. Получив доступ к администратору контроллера домена, злоумышленник получил доступ к хешированным паролям всех пользователей корпоративной сети. Пароли были слабые и не менялись с момента создания аккаунтов – злоумышленник без труда смог получить их исходные значения, подобрав пароли по радужным таблицам.

А. Выберите техники реализации угроз информационной безопасности из списка ниже, которые однозначно были использованы в приведенном эпизоде (исходя из приведенного описания инцидента)

|  |  |
| --- | --- |
|  | Спуфинг |
|  | **Кейлоггинг (создание кейлоггера)** |
|  | Тайпсквоттинг |
|  | Вишинг |
|  | Фишинг |
|  | **SQL-инъекция** |
|  | Межсайтовый скриптинг |
|  | **Эскалация привилегий** |
|  | **Несанкционированный доступ** |

Ответ А: (3 балла)

Б. Установите источник угрозы – внутренний или внешний. Ответ обоснуйте.

Ответ Б: Внешний

Участник должен привести в качестве обоснования ссылку на подтверждающий элемент в эпизоде.

Например: Да, является, потому что в описании инцидента указано, что исходящие сетевые соединения были осуществлены на IP-адрес частного хостинга, находящегося в государстве Т.

**Правильный ответ без обоснования 0 баллов**

**Правильный ответ с обоснованием 3 балла**

В. Определите ошибки, допущенные администратором системы, которые привели к сложившемуся инциденту безопасности, указать не менее трех

Ответ В: Ожидается, что участник должен перечислить следующие допущенные ошибки. За упоминание (в любом виде) ошибки начисляются баллы, максимально 3 балла:

1. Слабая парольная политика – администратор использовал один и тот же пароль на двух серверах, а пользователи сети использовал слабые пароли и не менял их с момента создания аккаунтов (1 балл)

2. Отсутствует патч-менеджмент – Munin был устаревшей версии с множеством уязвимостей. Необходимо было регулярно обновлять ПО до последней версии (1 балл)

3.Не установлено антивирусное ПО – злоумышленник успешно инфицировал контроллер домена своим кейлоггером (1 балл)

**За каждую 1 балл, максимально 3 балла**

**Количество баллов за задание – 10 баллов.**