Задания для муниципального этапа всероссийской олимпиады школьников по информатике и ИКТ, профиль «Информационной безопасности» для 9-11 классов, 2025/26 уч.год.

ВРЕМЯ ВЫПОЛНЕНИЯ: 180 МИНУТ.

Задание 1.

Клиент крупного банка, Владимир, собрался оплатить кредит через онлайн-банк. Он, как всегда, набрал в браузере «mybank.ru» и нажал «Enter.» Однако злоумышленник подменил IP-адрес легитимного сервера в DNS-ответе, направив пользователя на фальшивый сайт. Как называется такая атака?

Задание 2.

Операция «Тайный майнер: расследование компрометации сервера».

Вы — член команды SOC (Security Operations Center) компании *DataSafe*. В 14:30 по местному времени система мониторинга *SIEM* выдала серию «алертов» по ключевому серверу.

На сервере:

-резко вырос исходящий трафик;

-в процессах виден неизвестный процесс miner;

-в cron добавлены задания с подозрительными URL.

1. Опишите, что произошло?

2.Перечислите три шага по реагированию на инцидент информационной безопасности.

Задание 3.

Ответье на вопрос, какой файл в Linux хранит хеши паролей пользователей?

1./etc/passwd

2./etc/shadow

3./etc/group

4./etc/hosts

Задание 4.

Ответьте на вопрос**,** для чего используется стандарт **LUKS** в Linux?
1. Шифрование разделов диска.
2. Сжатие файлов.
3.Резервное копирование в облако.
4.Ускорение работы SSD.

Задание 5.

В логах сервера множество http-запросов с разными User-Agent, но одним IP-адресом. Каждый запрос содержит параметр ?id=1' OR '1'='1. Что это?
1.DDoS-атака.
2.Попытка SQL-инъекции.
3.Сканирование портов.
4.Фишинговая рассылка.

Задание 6.

Администратор сети выполняет в терминале Linux следующую команду:
ping -c 5 -i 2 -W 3 mail.ru

Опишите пошагово, что произойдёт при выполнении этой команды, и объясните значение каждой опции. Ответьте, какой вывод можно сделать по итоговой статистике, если получено 3 ответа из 5, среднее время отклика — 45 мс, а максимальное — 120 мс?

Требования к ответу:
1.Раскройте смысл каждой опции команды (-c, -i, -W).
2.Опишите последовательность действий утилиты ping при выполнении команды.
3.Проанализируйте приведённую статистику:
-что означает 3 ответа из 5?
-о чём говорит разброс времени отклика (45 мс vs 120 мс)?
-какие возможные причины таких результатов?

Задание 7.

Злоумышленник использует анализатор сетевого трафика Wireshark в сети с общим хабом (hub). Что он может получить?

1.Все пакеты, проходящие через хаб.

2.Только пакеты, адресованные его MAC.

3.Ничего — трафик зашифрован.

Задание 8.

Вы — специалист группы реагирования на инциденты в компании *SecureTech*. Вам поступил тревожный сигнал: в течение последних 2 часов наблюдаются аномалии в работе корпоративной сети.

Исходные данные:

1. Лог событий IDS/IPS(за период 14:00–16:00):

14:15:23 — [ALERT] Suspicious outbound connection to 185.123.45.67:443 (port scan pattern)
14:47:12 — [ALERT] SQL injection attempt on webserver (URL: /search?q=' OR 1=1--)
15:03:44 — [ALERT] Multiple failed SSH logins from 192.168.5.100 (5 attempts in 30 sec)
15:30:18 — [ALERT] Unusual DNS query volume (100+ requests/sec to random subdomains)

2. Отчёт системного администратора:

- На веб-сервере обнаружено изменение файла index.html (добавлена скрытая ссылка).
- В логах БД зафиксированы запросы на чтение таблицы users (10 000 строк).
- Несколько рабочих станций показывают высокую загрузку ЦП и сетевую активность.

3. Информация от пользователей:

- 3 сотрудника сообщили о «странных всплывающих окнах» в браузере.
- 1 пользователь заметил вход в почту с неизвестного устройства.

Задание:

1. **Выявите не менее 4 типов атак**, зафиксированных в логах и отчётах. Для каждой:

- укажите **название атаки** (термин);
- опишите **механизм реализации** (1–2 предложения);
- назовите **уязвимость/слабость**, которую использовал злоумышленник.

2. **Определите цепочку событий** (хронологию атак). Предположите, как злоумышленник мог продвигаться по сети (от начальной точки до финального действия).
3. **Предложите 3–4 срочные меры** для:

- остановки текущей атаки;
- локализации заражённых узлов;
- предотвращения повторного вторжения.

4. **Разработайте 2–3 долгосрочные меры** по усилению защиты:

- для веб-сервера;
- для почтовой системы;
- для рабочих станций.

Задание 9.

В упрощённой «азбуке Морзе» для цифр используются последовательности из точек (·) и тире (–) длиной ровно 4 символа. Например:

5.0 = · · · ·

6.1 = · – – –

Необходимо ответить на вопросы:

1. Сколько разных цифр можно закодировать такими последовательностями?
2. Можно ли добавить ещё одну цифру, не увеличивая длину кода?
3. Если для каждой цифры использовать ровно 5 символов, сколько цифр удастся закодировать?

Задание 10.

Вы — специалист по информационной безопасности компании *SecureNet*. Вам необходимо проанализировать текущую конфигурацию сетевого взаимодействия и предложить меры по усилению защиты данных.

Исходная ситуация:

В компании используются следующие сервисы и протоколы:
-веб-сайт (HTTP/HTTPS);
-почтовый сервер (SMTP, IMAP);
-удалённое администрирование (SSH);
-VPN для доступа сотрудников в корпоративную сеть.

При аудите выявлены следующие факты:

1.Веб-сайт частично работает по HTTP (некоторые страницы не перенаправляются на HTTPS).
2.На почтовом сервере используется устаревшая версия TLS 1.0.
3.Для SSH применяются ключи длиной 1 024 бита.
4.VPN-сервер использует протокол PPTP.
5.В сети не настроен механизм проверки сертификатов (OCSP/CRL).

Задание:

1.**Укажите уязвимости** в текущей конфигурации (по каждому из 5 пунктов). Кратко поясните, какие атаки возможны из-за каждой уязвимости (1–2 предложения).
2.**Предложите конкретные меры** по устранению каждой уязвимости.
Укажите:
- какие протоколы/версии следует использовать вместо текущих;
- какие параметры конфигурации нужно изменить (длины ключей, алгоритмы и т. п.);
- дополнительные механизмы защиты (если требуются).
3.**Объясните**, почему важно регулярно обновлять версии протоколов и алгоритмов шифрования. Приведите 2–3 аргумента.

Задание 11.

Вам представлены четыре сценария возможных инцидентов информационной безопасности и фрагменты логов/данных. **Определите:**
1. какой тип атаки реализован в каждом случае;
2. какую уязвимость использовал злоумышленник;
3. какие последствия возможны при успешной реализации атаки.

Известно, что среди ответов есть следующие виды атак: фишинг, SQL-инъекция, DDoS, компрометация учётной записи.

Для каждого сценария:

1.Назовите тип атаки (используйте общепринятые термины: фишинг, DDoS, SQL-инъекция, XSS, брутфорс, спуфинг и т. п.).

2.Укажите, какая уязвимость или слабое место системы позволило атаке состояться.
3.Опишите 1–2 возможных последствия (утечка данных, отказ сервиса, компрометация учётных записей и т. п.).
4.Предложите 1–2 меры защиты, которые могли бы предотвратить или снизить риск такой атаки.

Сценарии:

Сценарий 1. «Подозрительное письмо».

Пользователь получил письмо от «службы поддержки банка» с просьбой подтвердить данные карты по ссылке. Ссылка ведёт на сайт с адресом, похожим на официальный (например, bank-secure.net вместо bank.ru). При переходе на сайт требуется ввести номер карты, срок действия и CVV-код.

Сценарий 2. «Перегрузка сервера»

Администратор заметил резкий рост числа запросов к веб-серверу. Логи показывают тысячи соединений с разных IP-адресов, направленных на один эндпоинт /api/data. Сервер начал отвечать с задержками, затем перестал отвечать совсем.

Сценарий 3. «Странный запрос»

В логах веб-приложения обнаружен запрос:

GET /search?q=admin' OR '1'='1

После этого злоумышленник получил доступ к данным всех пользователей, включая пароли (хранились в незашифрованном виде).

Сценарий 4. «Неизвестный вход»

Пользователь обнаружил в истории входов в свой почтовый аккаунт запись:

- Устройство: iPhone 14;
- Местоположение: Токио, Япония;
- Время: 03:17 UTC (пользователь в это время спал в Москве).

Пароль от почты не менялся, двухфакторная аутентификация не включена.

Задание 12.

Напишите команду iptables, которая **запрещает** все входящие пакеты с IP-адреса 192.168.1.100.

Задание 13.

В 2021 году произошла крупная утечка паролей, известная как RockYou2021. В ней фигурировало около 8,4 млрд уникальных паролей, что стало на тот момент крупнейшей утечкой в истории. Файл с паролями объёмом около 100 ГБ был опубликован на хакерском форуме пользователем с ником RockYou2021. Эта утечка стала одним из крупнейших инцидентов того времени и подчеркнула важность защиты данных.

Вам предоставлен фрагмент лог-файла веб-сервера компании *SecureTech* за 12.03.2025:

192.168.1.100 - - [12/Mar/2025:14:23:15 +0300] "GET /login.php?user=admin' OR '1'='1 HTTP/1.1" 200 1245
192.168.1.100 - - [12/Mar/2025:14:23:18 +0300] "POST /login.php HTTP/1.1" 403 342
192.168.1.101 - - [12/Mar/2025:14:24:01 +0300] "GET /index.php?file=../../../../etc/passwd HTTP/1.1" 404 289
192.168.1.102 - - [12/Mar/2025:14:25:33 +0300] "GET / HTTP/1.1" 200 1567
192.168.1.100 - - [12/Mar/2025:14:26:02 +0300] "GET /api/data?id=<script>alert('XSS')</script> HTTP/1.1" 200 984

Задание:

1.Определите **тип каждой атаки**, зафиксированной в логах (всего 4 различные атаки). Кратко опишите механизм каждой из них (1–2 предложения).
2.Укажите, **какие уязвимости** веб-приложения позволили провести эти атаки.
3.Предложите **по 1–2 меры защиты** для каждой уязвимости (на уровне кода, конфигурации сервера или политик безопасности).
4.Объясните, почему код <script>alert('XSS')</script> в запросе может представлять угрозу, даже если страница отображается корректно.

Задание 14.

Робот по имени Эйдж «читает» QR-коды размером 3 × 3 клетки. Каждая клетка — либо чёрная (1), либо белая (0).

Ответьте на вопросы:

1. Сколько всего разных QR-кодов такого размера?
2. Сколько кодов, где ровно 4 чёрные клетки?

3. Робот понимает код, только если в нём есть хотя бы один «квадрат» 2×2 из чёрных клеток. Сколько таких кодов?
4. Придумайте правило кодирования, чтобы по коду 3×3 можно было однозначно определить цифру от 0 до 8 (всего 9 вариантов). Опишите правило и приведите примеры для 0, 1, 8.

Задание 15.

Для открытия сейфа нужно ввести четырехзначный код. Цифры могут повторяться. **Ответьте на следующие вопросы:**
1. Сколько всего существует возможных комбинаций кода для данных условий?
2. Сколько может быть возможных комбинаций, где все цифры разные?
3. Сколько комбинаций, где ровно две цифры одинаковые (остальные — разные)?
4.Сколько комбинаций, где цифры идут строго по возрастанию (например, 1234, 0125)?

Задание 16.

В адрес олимпиады по информационной безопасности пришло зашифрованное сообщение: Ф В М Е Ж Т И В Ф Ю

Найдите исходное сообщение, если известно, что шифрообразование заключалось в следующем. Пусть X_1, X_2 — корни трехчлена X^2+3X+1. К порядковому номеру каждой буквы в стандартном русском алфавите (33 буквы) прибавлялось значение многочлена $f(X)=X^6+3X^5+X^4+X^3+4X^2+3$, вычисленное либо при $X=X_1$, либо при $X=X_2$ (в неизвестном нам порядке), а затем полученное число заменялось соответствующей ему буквой.
Формат вывода: текстовое сообщение.

Задание 17.

Установите, можно ли создать проводную телефонную сеть связи, состоящую из 993 абонентов, каждый из которых был бы связан ровно с 99 другими.
Формат вывода: ДА/НЕТ.

Задание 18.

Чтобы запомнить периодически меняющийся пароль в ЭВМ, математики придумали следующий способ. При известном числе a (например, номере месяца в году), пароль представляет собой первые шесть цифр наименьшего решения уравнения:

$$a(x^2 - 1) = \sqrt{1 + \frac{x}{a}}, \text{ при } 0 < a < 1$$

Число меньшей значности дополняется справа необходимым числом нулей.
Решите такое уравнение при произвольном a>0.

Задание 19.

Буквы русского алфавите занумерованы в соответствии с таблицей.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Для зашифрования сообщения, состоящего их n букв, выбирается ключ К — некоторая последовательность из n букв приведенного выше алфавита. Зашифрование каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма.

Прочтите шифрованное сообщение: **Р Б Ь Н Т С И Т С Р Р Е З О Х**, если известно, что шифрующая последовательность не содержала никаких букв, кроме А,Б и В.

Формат вывода: осмысленное сообщение.

Задание 20.

Вам предоставлен **фрагмент дизассемблированного кода** (условный псевдоассемблер) и **краткое описание поведения** программы. Ваша задача — понять алгоритм работы и ответить на вопросы.

Фрагмент кода (с комментариями):

```
start:
    mov eax, [input_length]    ; загружаем длину введённой строки
    cmp eax, 8                 ; сравниваем с числом 8
    jne reject                 ; если не равно — переход к reject


    mov esi, input_string      ; указатель на введённую строку
    mov edi, secret_key        ; указатель на «секретный ключ»
    mov ecx, 8                 ; длина для сравнения — 8 байт
    rep cmpsb                  ; сравниваем 8 байт строки с secret_key
    jne reject                 ; если не совпадают — переход к reject


accept:
    call print_success         ; выводим сообщение об успехе
    jmp exit

reject:
    call print_failure         ; выводим «Access denied!»
    jmp exit


exit:
    ret
```

Описание поведения программы:

- Программа принимает на вход текстовую строку.
- Если строка **ровно 8 символов** и **совпадает с неким «секретным ключом»**, выводится сообщение об успехе.
- В противном случае выводится «Access denied!».

Задание

Ответьте на вопросы (кратко, по 1–3 предложения на каждый):

1. **Какова длина «правильного» входного значения?** Обоснуйте ответ, опираясь на код.
2. **Как программа проверяет совпадение введённой строки с «секретным ключом»?** Опишите последовательность действий (используйте названия команд из фрагмента).

3.**Что произойдёт, если ввести строку длиной 7 символов?** Какой участок кода будет выполнен и почему?

4.**Предположите, в каком виде может храниться** `secret_key` **в бинарном файле.** Где (в каких секциях PE/ELF) его можно попытаться найти?

5.**Назовите 2 инструмента**, которые помогут извлечь `secret_key` из исполняемого файла без запуска программы. Кратко поясните, как они работают в этом контексте.