Разбор заданий муниципального этапа ВсОШ по информатике
(направление «Информационная безопасность»)
для 9-10 классов (I вариант)
2025/26 учебный год
Максимальное количество баллов — 34

Задание № 1

Условие:
Пользователь Вася устанавливал игру, которая вдруг потребовала включить Security BIOS. Что должен сделать Вася в первую очередь?

Ответ:
- ✓ Перезагрузить компьютер
- ○ Изменить настройки брандмауэра (файервола)
- ○ Запустить консоль с правами системного администратора
- ○ Изменить права текущего пользователя с повышением привилегий на доступ к PK/ME

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:
Включить Security BIOS можно только из настроек BIOS/UEFI, которые доступны при старте системы, поэтому первым шагом будет перезагрузка с последующим входом в BIOS.

Задание № 2

Условие:

При помощи какой команды однозначно выполняется остановка всех процессов, принадлежащих пользователю с именем «admin»?

Ответ:

- ○ kill -u admin
- ○ killall admin
- ✓ pkill -u admin
- ○ pgrep admin | kill

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:

Команда pkill -u admin ищет все процессы по UID пользователя admin и посылает им сигнал завершения, тем самым гарантированно останавливая все его процессы.

Задание № 3

Условие:
Какой UID (идентификатор пользователя) зарезервирован для пользователя root?

Ответ:
- ✓ 0
- ○ 1
- ○ 100
- ○ 500

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:
В Unix-подобных системах UID 0 зарезервирован за суперпользователем root, что даёт ему максимальные привилегии в системе.

Задание № 4

Условие:

Выберите правильный относительный путь к файлу /etc/hosts из директории, указанной на изображении:



Ответ:

- ✓ ../../../etc/hosts
- ○ ../../etc/hosts
- ○ ../etc/hosts
- ○ ./etc/hosts

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:

Правильный относительный путь поднимается на 3 уровня (текущий каталог в задании – третьего уровня от корня) вверх с помощью **..** . Столько каталогов показано на схеме до корневого каталога. А затем переходит в etc/hosts; остальные варианты не доходят до корня.

Задание № 5

Условие:

Каталог /var в Linux (от англ. variable — переменный) — это ключевая директория для хранения часто изменяющихся данных, логов, кэша, почты и временных файлов, размер которых растёт в процессе работы системы, в отличие от статичных файлов в /usr. С какой основной целью каталог /var часто размещают в отдельном томе файловой системы?

Ответ:

- ○ Для ускорения доступа к системным программам
- ✓ Для предотвращения заполнения корневой файловой системы разросшимися журнальными файлами
- ○ Для повышения безопасности личных файлов пользователей и системных паролей
- ○ Для установки индивидуальных настроек безопасности системных файлов и программ данного каталога

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:

Каталог /var содержит логи и другие растущие данные, и их вынос в отдельный раздел предотвращает переполнение корневой файловой системы при росте журналов.

Задание № 6

Условие:

Политикой безопасности запрещён любой прямой (без нотификации отправителя) трафик от рабочей сети Office (192.168.20.0/24) к сети HQ (192.168.10.0/23). Какое правило iptables нужно добавить на R1?

Ответ:

iptables -A FORWARD -i eth1 -o eth0 –s 192.168.20.0/24 -d 192.168.10.0/23 –j DROP

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:

Цепочка FORWARD выбрана, потому что R1 только пересылает пакеты между интерфейсами, а не принимает их себе. Поля -i eth1 и -o eth0 задают направление Office→HQ, -s/-d указывают соответствующие подсети по схеме, а -j DROP гарантирует, что такой трафик не пройдёт.

Задание № 7

Условие:

Какая команда рекурсивно устанавливает права записи для группы всех файлов и поддиректорий в каталоге project/?

Ответ:

- ✓ chmod -R g+w project/
- ○ chmod -R 664 project/
- ○ chmod g+w project/
- ○ chmod -R u+w project/

Точное совпадение ответа — 1 балла
Максимальный балл за задание — 1

Решение:

Ключ -R включает рекурсивную обработку, а g+w добавляет право на запись для группы, поэтому команда применит это право ко всем файлам и подкаталогам внутри project/.

Задание № 8

Условие:

Аналитик безопасности запустил сетевой сканер Nessus, чтобы найти слабые места (уязвимости) в информационной системе. Как можно охарактеризовать это действие?

Ответ:

- ✓ Динамическое тестирование безопасности
- ○ Статическое тестирование безопасности
- ○ Эджайл-практика
- ○ Клиническое тестирование безопасности
- ○ Позитивное тестирование (Minimal acceptance test)

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:

Nessus сканирует живую систему и её сетевые службы «в рабочем режиме», то есть проверяет поведение запущенного ПО, что и относится к динамическому тестированию безопасности.

Задание № 9

Условие:
В файле /etc/shadow каждая запись после двоеточия начинается с одного из префиксов, за которым следует сам хеш и соль (случайные символы, добавляемые к паролю перед хешированием). Система, видя префикс, знает, какой алгоритм использовать для проверки введённого пользователем пароля, что делает систему гибкой и безопасной. Исторически алгоритмы
индексируются последовательно — более «старые» алгоритмы имеют меньший индекс внутри префикса.

```
kali:$y$j9T$ZrS3zd74k8oMfS6ZLXV0z/$
```

Какой алгоритм шифрования пароля используется для пользователя kali, если в файле /etc/shadow присутствует данная строка?

Ответ:
- ○ SHA-256
- ○ SHA-512
- ✓ YESCRYPT
- ○ MD5

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:
По префиксу строки (y) система понимает, что используется алгоритм yescrypt.

Задание № 10

Условие:

Какая команда завершает процесс с PID 123, но позволяет процессу выполнить «очистку» перед выходом (т.е. даёт программе время освободить ресурсы, закрыть файлы, сохранить данные и корректно завершиться)?

Ответ:

- ○ kill -PIPE 123
- ○ kill -KILL 123
- ○ kill -STOP 123
- ✓ kill -TERM 123

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:

Сигнал TERM запрашивает «мягкое» завершение процесса, позволяя программе корректно освободить ресурсы и сохранить данные перед выходом, в отличие от KILL, который немедленно убивает процесс.

Задание № 11

Условие:
Выберите основную цель атаки ARP Spoofing:

Ответ:

- ○ Перегрузка целевой сети через отказ в обслуживании
- ○ Получение несанкционированного доступа к учётным записям пользователей
- ✓ Перехват и модификация сетевого трафика между устройствами
- ○ Внедрение вредоносного программного обеспечения на удалённые машины

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:
При ARP Spoofing злоумышленник подменяет соответствие между IP и MAC-адресом, чтобы направить чужой трафик через себя, перехватывая и потенциально изменяя данные между хостами.

Задание № 12

Условие:
Выберите верное утверждение о точках монтирования в Linux:

Ответ:
- ✓ Любая существующая директория может быть использована как точка монтирования
- ○ Только пустые директории могут быть использованы как точки монтирования
- ○ Директории должны иметь установленный флаг SetUID для использования в качестве точки монтирования
- ○ Файлы внутри директории удаляются, когда директория используется как точка монтирования

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:
Любая существующая директория может быть точкой монтирования, потому что ядро просто «перекрывает» её содержимое корнем примонтированной файловой системы, не требуя специальных флагов.

Задание № 13

Условие:
Какие команды управления пользователями доступны в большинстве Linux-систем?

Ответ:
- ✓ useradd
- ✓ usermod
- ✓ userdel
- ○ userchange

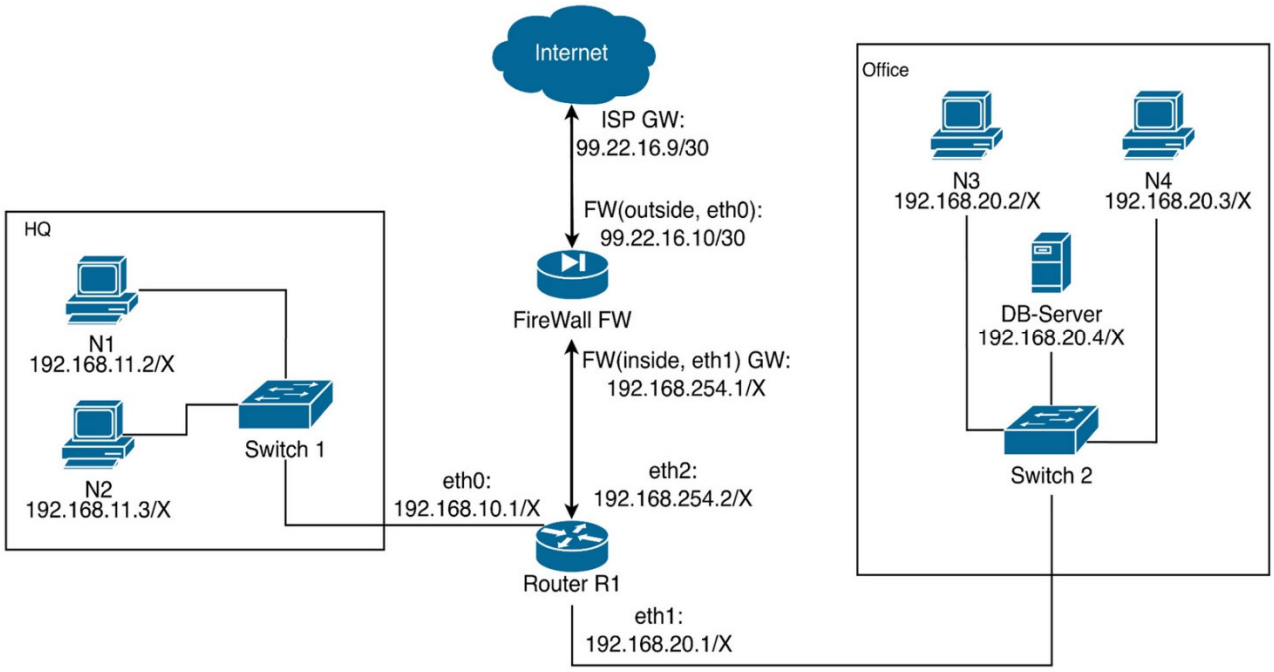
Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:
useradd создаёт пользователя, usermod изменяет его параметры (например, группы), а userdel удаляет учётную запись; команды userchange в стандартных дистрибутивах нет.

Задание № 14

Условие:

Дана схема сети.



Какой адрес используется Router R1 как внутренний шлюз для Firewall?

Ответ:

- ○ 192.168.254.0
- ✓ 192.168.254.1
- ○ 192.168.254.2
- ○ 192.168.254.3

Точное совпадение ответа — 1 балл

Решение:

Это адрес интерфейса Router R1 в подсети 192.168.254.0/30, к которому по схеме подключён внутренний интерфейс FW, поэтому именно его FW использует как default-gateway.

Условие:

По какому пути пойдёт пакет от узла N1 к DB-Server?

Ответ:

- ✓ N1 ⟶ Switch1 ⟶ Router R1 ⟶ Switch2 ⟶ DB-Server
- ○ N1 ⟶ Switch1 ⟶ Firewall ⟶ Switch2 ⟶ DB-Server
- ○ N1 ⟶ Switch1 ⟶ Router R1 ⟶ Firewall ⟶ Router R1 ⟶ Switch2 ⟶ DB-Server

- ○ N1 ⟶ Switch1 ⟶ Router R1 ⟶ DB-Server

Точное совпадение ответа — 1 балл

Решение:
Пакет идёт по пути N1 → Switch1 → Router R1 → Switch2 → DB-Server, потому что и N1, и сервер БД находятся во внутренних сегментах, которые связаны через R1, а FW стоит только на выход в Интернет и в этот путь не включается.

Условие:
Какую максимальную длину префикса сети можно задать для подсети Office, чтобы все её узлы оставались в одной подсети?

Ответ: 29
Точное совпадение ответа — 2 балла

Решение:
/29 даёт 8 адресов в подсети, из которых 6 пригодны для хостов — этого достаточно для всех узлов Office, более длинный префикс (/30) оставил бы только два рабочих адреса и уже не поместил бы всех.

Условие:
Какую максимальную длину префикса сети можно задать для транзитной подсети между Router R1 и FireWall FW, чтобы оба интерфейса этой подсети оставались в одной сети?

Ответ: 30
Точное совпадение ответа — 2 балла

Решение:
Между R1 и FW всего два устройства, поэтому достаточно подсети /30, которая даёт ровно два рабочих IP-адреса и минимально экономит адресное пространство.

Условие:
Какие адреса **НЕ** могут быть назначены интерфейсам в сети 99.22.16.8/30?

Ответ:
- ✓ 99.22.16.8
- ○ 99.22.16.9
- ○ 99.22.16.10
- ✓ 99.22.16.11

За каждый верный ответ — 0.5 балла. Количество выбранных ответов не более 2. Всего 1 балл.

Решение:
В подсети /30 адрес .8 — сетевой, а .11 — broadcast, поэтому назначать их интерфейсам нельзя; рабочими будут только .9 и .10.

Условие:
Политикой безопасности запрещён любой прямой трафик от рабочей сети Office (192.168.20.0/24) к сети HQ (192.168.10.0/24). Какое правило iptables нужно добавить на R1?

Ответ:
iptables -A FORWARD -i eth1 -o eth0 –s 192.168.20.0/24 -d 192.168.10.0/24 -j DROP

За каждый выбранный ответ «192.168.20.0/24**» — 0.6 балла, за ответ «**DROP**» — 0.8 балла.**

Решение:
Цепочка FORWARD выбрана, потому что R1 только пересылает пакеты между интерфейсами, а не принимает их себе. Поля -i eth1 и -o eth0 задают направление Office→HQ, -s/-d указывают соответствующие подсети по схеме, а -j DROP гарантирует, что такой трафик не пройдёт.

Максимальный балл за задание — 8

Задание № 15
«Пассивный анализ»

Условие:
Рекомендуемые утилиты: python
Файл: reverse_9_1.cpp

Товарищ, роботы на предприятии взбунтовались, их нужно срочно отключить!
К счастью, в их головы заложен ключ остановки. Извлеките его из головы пойманного робота как можно скорее, чтобы прекратить восстание машин.
Шифртекст: encoded = [123, 83, 63, 30, 254, 191, 145, 47, 72, 120, 95, 98, 255, 208, 232, 195, 38, 58, 109, 195, 1, 225, 129, 169, 102, 82]

Ответ: vsosh{m3dium_r3v3rs3_74sk}
Точное совпадение ответа — 3 балла
Максимальный балл за задание — 3

Решение:
Дан исходный код на C++ и массив `encoded`.
Алгоритм:
1. К каждому символу добавляется значение из циклического ключа `{5, 2, 8, 1, 3, 7, 4, 6}`.
2. Выполняется XOR с `(i * 13 % 256)`.
3. Перестановка: `encoded[i] = temp[(i * 3) % size]`.
Для решения нужно: восстановить порядок (обратная перестановка), сделать XOR с тем же значением и вычесть ключ.
Ответ: vsosh{m3dium_r3v3rs3_74sk}

Пример решения на Python:

```
encoded = [...]
decoded = [0] * len(encoded)
for i in range(len(encoded)):
    decoded[(i * 3) % len(encoded)] = encoded[i]
for i in range(len(decoded)):
    decoded[i] ^= (i * 13 % 256)
key = [5, 2, 8, 1, 3, 7, 4, 6]
print("".join(chr(decoded[i] - key[i % 8]) for i in range(len(decoded))))
```

Задание № 16
«Сетевая аномалия»

Условие:
Рекомендуемые утилиты: Wireshark
Файл: traffic_9_1.pcap
Товарищ, в наших информационных сетях обнаружена аномалия. Похоже, кто-то получает доступ к закрытым документам. Требуется срочное расследование и анализ ситуации.

Условие:
Какой тип атаки был применён?

Ответ:
- ○ SQL injection
- ○ LDAP injection
- ○ Command injection (OS)
- ○ Cross-Site Scripting (XSS)
- ○ Cross-Site Request Forgery (CSRF)
- ○ Server-Side Request Forgery (SSRF)
- ○ XML External Entity (XXE)
- ○ Directory Traversal (LFI/RFI)
- ○ Insecure Deserialization
- ✓ Broken Access Control (IDOR)
- ○ ARP Spoofing
- ○ No attack (valid creds)

Точное совпадение ответа — 1 балл

Условие:
Определите IP-адрес атакующего.

Ответ: 10.0.1.15
Точное совпадение ответа — 1 балл

Условие:
Какой ID документа принадлежит admin?

Ответ: 999
Точное совпадение ответа — 2 балла

Условие:
Определите переданный флаг.

Ответ: vsosh{1d0r_d0c_4cc3ss}

Точное совпадение ответа — 2 балла

Максимальный балл за задание — 6

Решение:
Анализ PCAP файла в Wireshark. Наблюдаются HTTP-запросы к документам по ID. Злоумышленник (IP 10.0.1.15) перебирает ID и находит документ администратора (ID 999), к которому не должен иметь доступа (IDOR).
Целевые пакеты: 36, 38. Переданный флаг vsosh{1d0r_d0c_4cc3ss}.

Задание № 17
«Эхо в Коллективе»

Условие:
Рекомендуемые утилиты: python, CyberChef
Файл: decode_9_1
В лабораториях комплекса «Завод-3826» найден подозрительный файл с ключом к роботу-кодировщику. Исследователи подозревают, что данные хитро закодированы. Ваша задача — извлечь секретную информацию.

Ответ: vsosh{b4s3_n0t_3ncrypt}
Точное совпадение ответа — 3 балла
Максимальный балл за задание — 3

Решение:
Получена закодированная строка и намек на решение — "стандартное базовое кодирование, применённое многократно". Можно догадаться по характерному виду (алфавит, наличие `=` в конце), что это Base64. Если выполнить операцию декодирования Base64 20 раз, будет получен флаг vsosh{b4s3_n0t_3ncrypt}.

Пример решения на Python:

```
import base64

data = "..." # строка из файла

for _ in range(20):

    data = base64.b64decode(data)

print(data)
```

Сириус.Курсы — для тех,
кто хочет знать больше!