Разбор заданий муниципального этапа ВсОШ по информатике
(направление «Информационная безопасность»)
для 9-10 классов (II вариант)

2025/26 учебный год

Максимальное количество баллов — 34

Задание № 1

Условие:

Какие **два** параметра можно настроить через BIOS?

Ответ:

- ✓ Порядок загрузочных устройств
- ○ Версия ядра Linux
- ✓ Конфигурация оборудования
- ○ Имя узла (host) системы
- ○ Открытые/закрытые порты подключения к узлу

Точное совпадение ответа — балл

Максимальный балл за задание — 1

Решение.

В BIOS настраивают порядок загрузочных устройств (например, сначала USB, потом диск) и включают/отключают оборудование (встроенные контроллеры, порты), а не параметры ОС вроде ядра или hostname.

Задание № 2

Условие:

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 упрощения процесса обновления системы

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Решение.

Журналы и кэш в /var могут быстро расти, и отдельный раздел защищает корневую файловую систему от переполнения из-за этих файлов.

Задание № 3

Условие:

С помощью какой команды выполняется добавление пользователя с именем «petr» в группу «wheel»?

Ответ:

- ○ groupadd petr wheel
- ○ uadd petr wheel
- ○ passwd -G wheel petr
- ✓ usermod -aG wheel petr

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

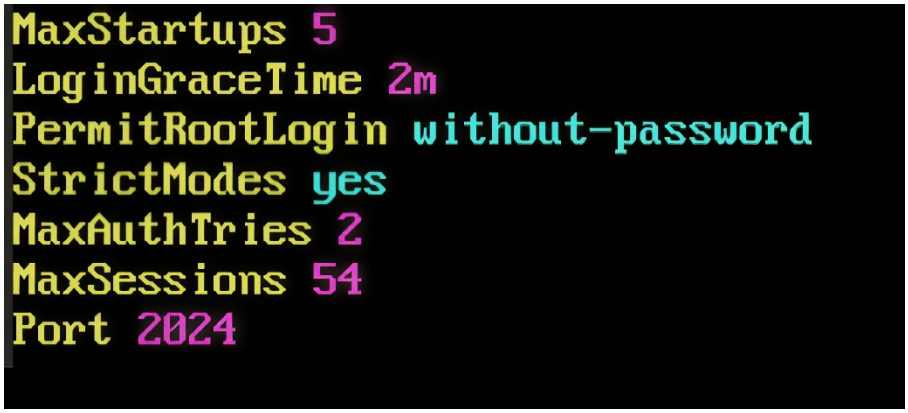
Решение.

Как и в предыдущем случае, usermod -aG wheel petr добавляет пользователя petr в группу wheel, не трогая его текущие группы.

Задание № 4

Условие:

На изображении представлено содержание файла конфигурации SSH-сервера (sshd_config).



Какое максимальное количество одновременных SSH-сессий разрешено в данной конфигурации?

Ответ:

- ○ 2
- ○ 5
- ✓ 54
- ○ 2024

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Решение.

Максимальное число одновременных SSH-сессий берётся из параметра MaxSessions (или аналогичного), поэтому правильный ответ — то значение, которое указано напротив этого параметра в конфигурации.

Задание № 5

Условие:

Какая команда может быть использована для создания загрузочного USB-носителя из образа диска в операционной системе Linux?

Ответ:

- ○ gdisk
- ✓ dd
- ○ cc
- ○ fdisk
- ○ mount

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Решение.

Утилита dd умеет поблочно копировать образ диска (ISO) на устройство /dev/sdX, что и используется для создания загрузочного USB-носителя.

Задание № 6

Условие:

Определите объём доступного пространства на разделе /dev/sda2 согласно выводу команды df –m:

```
Filesystem     1M-blocks  Used Available Use% Mounted on
udevfs                 5     1         5   2% /dev
runfs                229     1       229   1% /run
/dev/sda2          14778  2760     11246  20% /
tmpfs                229     0       229   0% /dev/shm
tmpfs                229     0       229   0% /tmp
tmpfs                 46     0        46   0% /run/user/0
```

Ответ:

- 11246 B
- 2760 Mb
- ✓ 11246 Mb
- 14778 Mb

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Решение.

В выводе df -m нужно смотреть колонку Available (или Avail) напротив строки /dev/sda2; именно это число в мегабайтах и соответствует искомому объёму.

Задание № 7

Условие:

Какая команда выведет последние 15 строк текстового файла?

Ответ:

- ○ cat -n 15 txt
- ○ dump -n 15 txt
- ○ head -n 15 txt
- ✓ tail -n 15 txt

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Решение.

Команда tail -n 15 txt выводит последние 15 строк файла, тогда как head показывает начало, а cat — весь файл целиком.

Задание № 8

Условие:

При расследовании инцидентов безопасности в первую очередь обращаются к истории команд пользователей. Какой файл в домашнем каталоге пользователя используется для хранения истории команд Bash?

Ответ:

- ✓ bash_history
- ○ bash_histfile
- ○ history
- ○ bashrc_history
- ○ history_bash

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Решение.

История команд Bash по умолчанию хранится в скрытом файле ~/.bash_history, именно его и анализируют при расследовании инцидентов.

Задание № 9

Условие:

Установите соответствие между сетевыми протоколами и их отличительными особенностями.

Ответ:

FTPS	Стандартный FTP с поддержкой SSL/TLS
FTP	Передаёт данные в открытом виде, порты 20/21
TFTP	Простой протокол без аутентификации, порт 69
SFTP	Использует SSH для шифрования, порт 22

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

Решение.

FTP (1→a) работает по портам 20/21 и передаёт данные в открытом виде; SFTP (2→b) использует SSH по 22 порту и шифрует всё; FTPS (3→c) добавляет SSL/TLS к FTP; TFTP (4→d) — упрощённый протокол без аутентификации по UDP-порту 69.

Задание № 10

Условие:

Протокол HTTPS реализует, в первую очередь, передачу гипертекстовой разметки. Поверх какого транспортного протокола (обычно) он функционирует?

Ответ:

- ○ ICMP
- ✓ TCP
- ○ UDP
- ○ TLS/SSL

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Решение.

HTTPS — это HTTP поверх TLS, который, в свою очередь, использует транспортный протокол TCP, поэтому транспортный уровень здесь именно TCP.

Задание № 11

Условие:

Перед администратором стоит задача проверить доступность веб-сервера (IP: 192.168.4.46) на узле, не имеющем графического интерфейса. Какую команду он использует?

Ответ:

- ○ web-client 192.168.4.46
- ○ http://192.168.4.46
- ○ mozila.sh 192.168.4.46
- ✓ curl 192.168.4.46

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

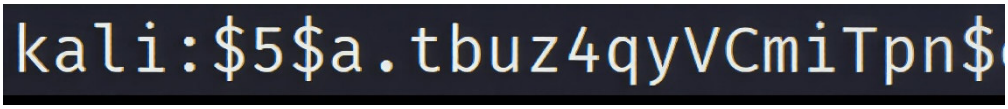
Решение.

curl 192.168.4.46 отправляет HTTP-запрос к серверу и выводит ответ прямо в терминал, что удобно для проверки доступности и работы веб-службы.

Задание № 12

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. Алгоритмы нумеруются последовательно — более «старые» алгоритмы имеют меньший индекс внутри префикса.



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

Ответ:

- ✓ SHA-256
- ○ SHA-512
- ○ yesscript
- ○ MD5

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Решение.

- Префикс вида 5 в hash-строке у пользователя kali соответствует алгоритму SHA-256, а, например yesscript имеет префикс y или 7. Даже если не помнить такие детали, ответ на вопрос можно получить (при знании того, что префиксы обозначают тип хэш-функции) методом рассуждений. Более ранние алгоритмы имеют меньшее значение цифры в префиксе (т.к. добавлялись в ОС Linux последовательно). Поэтому yesscript (как самый новый) и MD5 (как самый старый) можно отмести сразу.

.

Задание № 13

Условие:

Администратор сети в терминале ввёл команду и получил результат, представленный на изображении.



Какую команду он использовал?

Ответ:

- ○ ssh-copy-id
- ○ ssh-keyscan
- ○ ssh-genrsa
- ✓ ssh-keygen

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

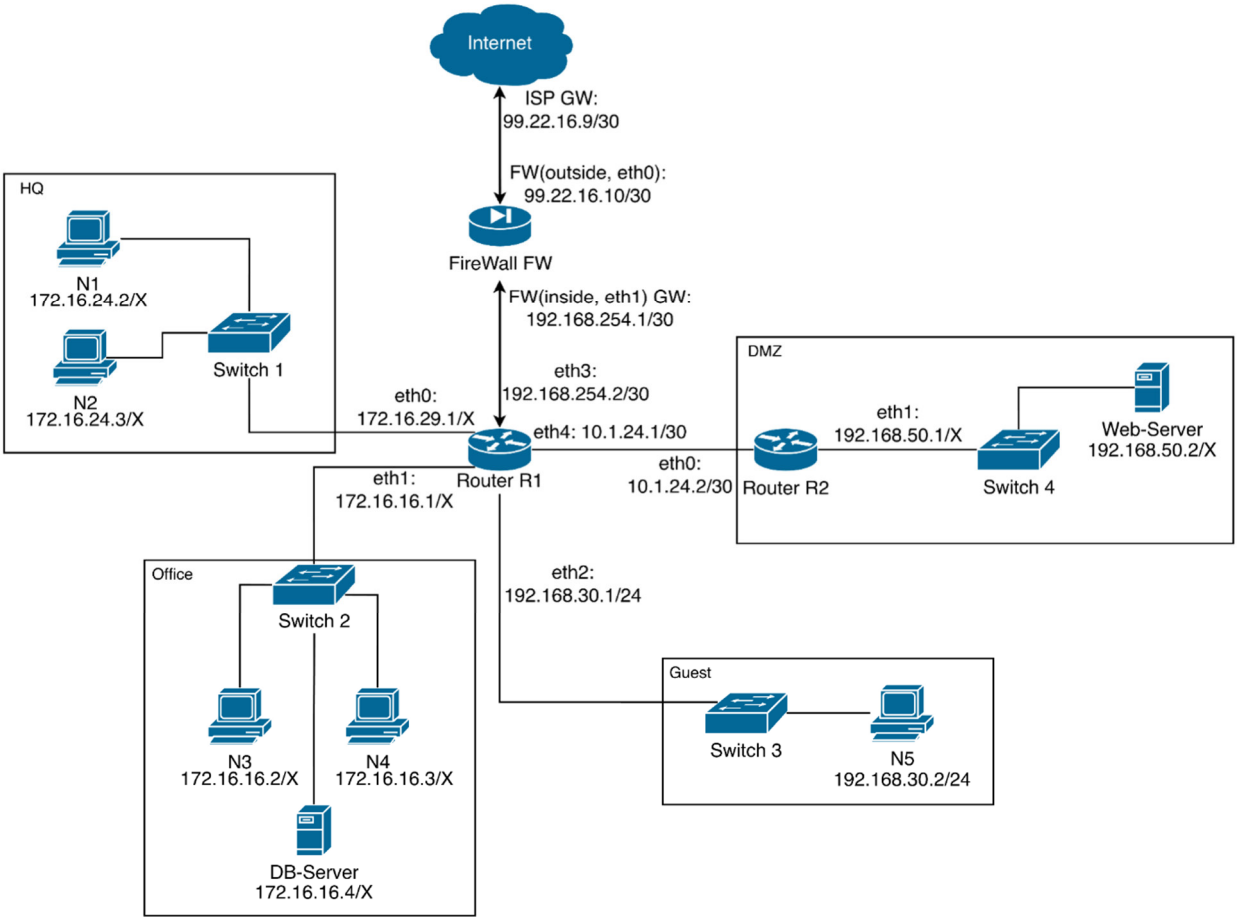
Решение.

ssh-keygen генерирует пару SSH-ключей и в выводе показывает путь к созданным файлам и отпечаток ключа, что и видно на типичных скриншотах.

Задание № 14

Общее условие:

Дана схема сети.



Условие:

Какие сети напрямую подключены к Router R1?

Ответ:

- ✓ 172.16.29.0
- ✓ 172.16.16.0
- ✓ 192.168.30.0
- ○ 192.168.50.0
- ✓ 192.168.254.0
- ✓ 10.1.24.0

За каждый верный ответ — 0.2 балла. Всего 1 балл. Количество выбранных ответов не более 5.

Решение.

К R1 непосредственно подключены сети HQ 172.16.24.0/21, Office 172.16.16.0/29, гостевая 192.168.30.0/24 и линк 10.1.24.0/30 — у маршрутизатора есть интерфейсы в этих подсетях, а DMZ 192.168.50.0/24 лежит за FW.

Условие:

Выберите broadcast-адрес WAN-сети 99.22.16.8/30:

Ответ:

- 99.22.16.8
- 99.22.16.9
- 99.22.16.10
- ✓ 99.22.16.11

Точное совпадение ответа — 1 балл

Решение.

В /30-сети 99.22.16.8–99.22.16.11 последний адрес (.11) является широковещательным, а два средних (.9 и .10) используются на линке.

Условие:

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

Ответ: 29

Точное совпадение ответа — 1 балл

Решение.

/29 даёт минимум IP-адресов, которых всё ещё хватает для всех хостов сегмента Office.

Условие:

Чтобы Router R1 знал путь в сеть 192.168.50.0/24 (DMZ), нужно добавить маршрут. Какой вариант ip route соответствует требованию?

ip route add...

Ответ:

- 10.1.24.0/30
- 172.16.24.0/21
- 172.16.16.0/24
- ✓ 192.168.50.0/2

Точное совпадение ответа — 0.6 балла

...via...

Ответ:

- ✓ 10.1.24.2
- 99.22.16.9
- 192.168.50.1
- 192.168.254.1

Точное совпадение ответа — 0.6 балла

...dev...

Ответ:

- ○ eth1
- ○ eth2
- ○ eth3
- ✓ eth4

Точное совпадение ответа — 0.8 балла

Решение.

Здесь 192.168.50.0/24 — сеть назначения DMZ, которую R1 сам напрямую не знает; via 10.1.24.2 указывает следующий хоп (адрес FW в общей с R1 подсети), а dev eth4 фиксирует, через какой интерфейс R1 физически отправлять пакеты к этому next-hop.

Условие:

Какой шлюз по умолчанию будет настроен для N1?

Ответ: 172.16.29.1

Точное совпадение ответа — 2 балла

Решение.

Для узла N1 default-gateway берётся адрес роутера в его локальной подсети 192.168.29.0/24 — это 192.168.29.1, через который он выходит во все другие сети.

Условие:

Нужно разрешить доступ к Web-Server (192.168.50.2) из Интернета по протоколам HTTP и HTTPS. Какое правило iptables в цепи FORWARD нужно добавить на FW?

iptables -A FORWARD -i eth0 –p...

Ответ:

- ✓ tcp
- ○ udp
- ○ icmp
- ○ all

Точное совпадение ответа — 0.5 балла

...-m multiport –dports...

Ответ:

- ○ 21
- ○ 25
- ○ 53
- ✓ 80

Точное совпадение ответа — 0.5 балла

Ответ:

- ○ 22
- ○ 67
- ○ 110
- ✓ 443

Точное совпадение ответа — 0.5 балла

...-d 192.168.50.2 -j ...

Ответ:

- ✓ ACCEPT
- ○ DROP
- ○ REJECT
- ○ LOG

Точное совпадение ответа — 0.5 балла

Максимальный балл за задание — 9

Решение.

FORWARD выбран, так как речь о маршрутизации между подинтерфейсами (VLAN), -i eth0.10 и -o eth0.20 задают направление трафика из VLAN10 в VLAN20, а цель -j ACCEPT разрешает такое перенаправление.

Задание № 15

Условие:

Рекомендуемые утилиты: Python

Файл: reverse_9_2.cpp

Сигнал тревоги на космической станции был зашифрован, чтобы враги не смогли понять инструкции. Кажется, кто-то изменил порядок команд с помощью хитрого алгоритма. Расшифруйте послание и восстановите правильную последовательность действий, чтобы спасти станцию.

Шифртекст:

encoded = [118, 106, 129, 104, 129, 103, 109, 112, 102, 97, 120, 56, 126, 55, 115, 122, 54, 97, 61, 57, 123, 111, 126, 122, 116, 118]

Ответ: vsosh{cyclic_r3v3rs3_74sk}

Точное совпадение ответа — 3 балла

Максимальный балл за задание — 3

Решение.

Алгоритм:

1. Сложение с ключом `{4, 1, 7, 3, 2, 6, 5, 8}` по модулю 256.
2. Циклический сдвиг массива на 3 позиции вправо.

Для решения: сдвиг влево на 3 и вычитание ключа.

Ответ: `vsosh{cyclic_r3v3rs3_74sk}`

Пример решения на Python:

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

Задание № 16

Общее условие:
Рекомендуемые утилиты: Wireshark
Файл: traffic_9_2.pcap
Товарищ, в наших информационных сетях обнаружена аномалия. Похоже, кто-то пытается взломать базу данных интернет-магазина. Требуется срочное расследование и анализ ситуации.

Условие:
Какой тип атаки был применён?

Ответ:

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

Точное совпадение ответа — 1 балл

Условие:
Определите IP-адрес атакующего.

Ответ: 10.0.2.20
Точное совпадение ответа — 1 балл

Условие:
Из какой таблицы злоумышленник получил данные?

Ответ: users
Точное совпадение ответа — 1 балл

Условие:
Определите переданный флаг.

Ответ: vsosh{sql_1nj3ct_m4st3r}

Точное совпадение ответа — 3 балла
Максимальный балл за задание — 6

Решение.
В трафике видны классические признаки SQL-инъекции в параметрах HTTP-запроса от атакующего (IP 10.0.2.20). Злоумышленник извлекает данные из таблицы `users`.
Целевые пакеты: 38, 40, 42, 44, 46.
1. Тип атаки: SQL injection
2. IP атакующего: 10.0.2.20
3. Таблица: users
4. Флаг: vsosh{sql_1nj3ct_m4st3r}

Задание № 17

Условие:

Рекомендуемые утилиты: Python, CyberChef

Файл: decode_9_2

В лабораториях комплекса «Завод-3826» найден подозрительный файл с ключом к роботу-кодировщику. Исследователи подозревают, что данные хитро закодированы какое-то количество раз; возможно, применялась и не одна кодировка.

Ваша задача — извлечь секретную информацию.

Ответ: vsosh{h3x_th3n_b43d}

Точное совпадение ответа — 3 балла

Максимальный балл за задание — 3

Решение.

Двойное кодирование: сначала данные были закодированы в Base64, а затем результат представлен в виде Hex-строки. Нужно сначала перевести Hex в байты, затем декодировать Base64.

Ответ: `vsosh{h3x_th3n_b43d}`

Пример решения на Python:

```
import base64
data = "..." # hex string
b64_data = bytes.fromhex(data)
print(base64.b64decode(b64_data))
```

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

