Задания **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:
- o 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

Задание № 2

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

Ответ:
- ○ kill -u admin
- ○ killall admin
- o pkill -u admin
- ○ pgrep admin | kill

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

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

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

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

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:

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

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

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

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

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

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

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

Задание № 13

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

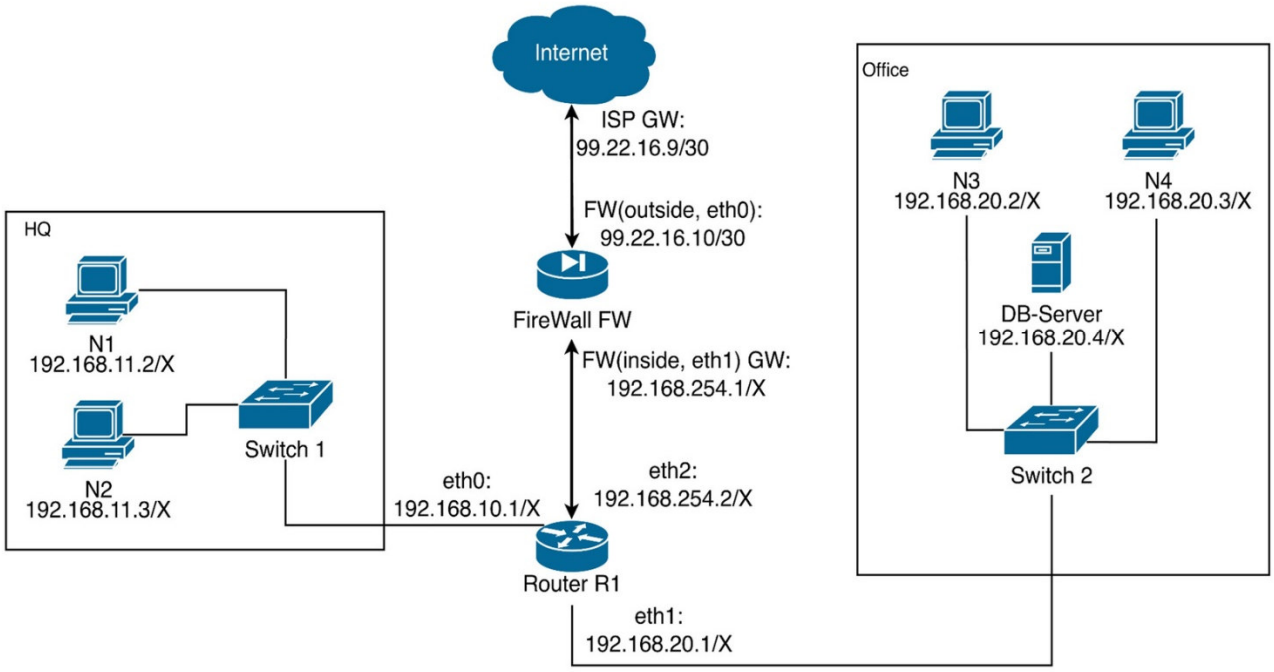
Ответ:
- useradd
- usermod
- userdel
- userchange

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

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

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

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

Ответ:
Точное совпадение ответа — 2 балла

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:
Точное совпадение ответа — 2 балла

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.

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:

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

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

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:
Точное совпадение ответа — 1 балл

Условие:
Какой ID документа принадлежит admin?

Ответ:
Точное совпадение ответа — 2 балла

Условие:
Определите переданный флаг.

Ответ:

Точное совпадение ответа — 2 балла

Максимальный балл за задание — 6

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)
```