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

Задание № 1

Условие:
Аналитик безопасности запустил сканер программного кода (white box), чтобы найти слабые места (уязвимости) в информационной системе. Как можно охарактеризовать это действие?

Ответ:
- ○ Динамическое тестирование безопасности
- ✓ Статическое тестирование безопасности
- ○ Smoke-тестирование
- ○ Проверка конфиденциальности
- ○ Клиническое тестирование безопасности

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

Решение:
Сканер исходного кода анализирует программы без их запуска, что и относится к статическому тестированию безопасности, в отличие от динамического анализа.

Задание № 2

Условие:
Какие три модели являются основой облачных технологий?

Ответ:
- ○ HaaS, DaaS, WaaS
- ○ IaaS, CaaS, SaaS
- ✓ IaaS, PaaS, SaaS
- ○ PaaS, SaaS, EaaS

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

Решение:
Эти три модели описывают базовые уровни облачных услуг: инфраструктура как услуга, платформа как услуга и программное обеспечение как услуга.

Задание № 3

Условие:
В чём заключается основная причина отказа применения протокола Telnet в локальных и публичных сетях?

Ответ:
- ○ Низкая скорость
- ✓ Отсутствие механизмов шифрования
- ○ Отсутствие совместимости с новыми ОС
- ○ Технически сложная настройка

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

Решение:
Telnet передаёт логины, пароли и данные в открытом виде, без шифрования, что делает его небезопасным в современных сетях.

Задание № 4

Условие:

Администратору сети Linux необходимо присвоить права на исполнение файла /etc/start.up. При помощи какой команды он может это сделать?

Ответ:

- ○ chmod a-x /etc/start.up
- ○ chmod g=u /etc/start.up
- ✓ chmod u+x /etc/start.up
- ○ chmod u /etc/start.up

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

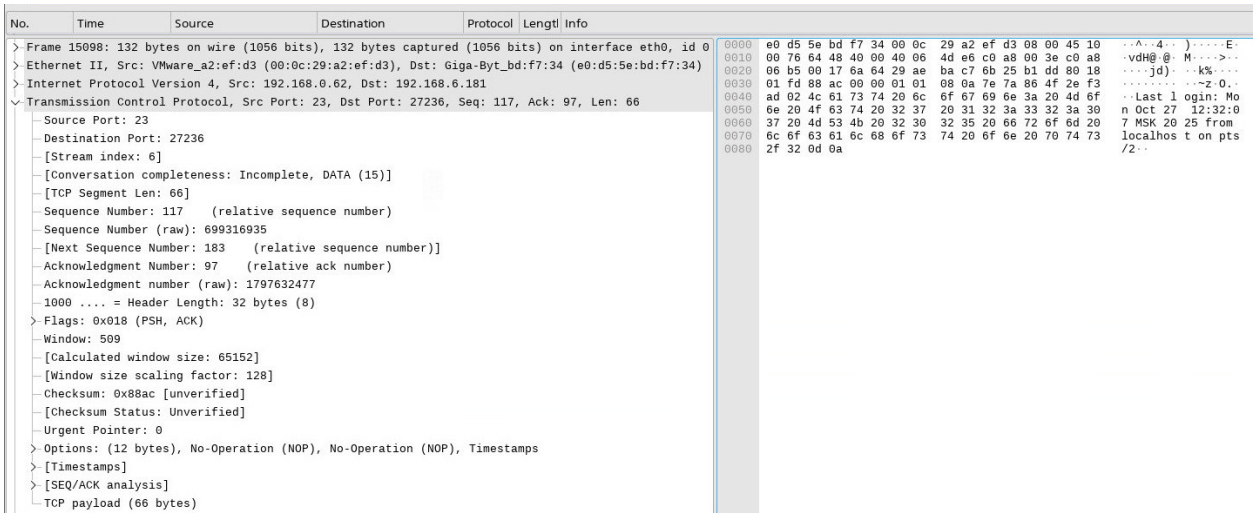
Решение:

Ключ u+x добавляет право на выполнение для владельца файла, поэтому скрипт может быть запущен как программа пользователем-владельцем.

Задание № 5

Условие:

На изображении представлен дамп сетевого пакета. По какому протоколу осуществляется взаимодействие между клиентом и сервером?



Ответ:

- ○ ssh
- ✓ telnet
- ○ ftp
- ○ sftp

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

Решение:

В дампе обычно видно использование порта 23 и нешифрованный обмен, что характерно для протокола Telnet. По умолчанию Telnet использует исходящий (и входящий) порт 23 (TCP).

Задание № 6

Условие:

При анализе ARP-таблицы (кэша) обнаружена запись с IP-адресом 192.168.1.100.

```
┌──(kali㉿kali)-[~]
└─$ ip neighbour show
10.0.2.2 dev eth0 lladdr 52:55:0a:00:02:02 REACHABLE
192.168.1.100 dev eth0 INCOMPLETE
fe80::2 dev eth0 lladdr 52:56:00:00:00:02 router STALE
fd17:625c:f037:2::2 dev eth0 lladdr 52:56:00:00:00:02 router STALE
```

Какие утверждения верно описывают данную запись?

Ответ:

- ○ Запись корректна и в данный момент используется
- ✓ ARP-запрос отправлен, но ответ на него ещё не поступил
- ○ ARP-запрос неполон и небезопасен
- ○ Срок записи истёк, и она подлежит удалению
- ○ Запись требует проверки, признаки ARP-Spoofing

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

Решение:

При статусе вида incomplete видно, что ARP-запрос на IP 192.168.1.100 был отправлен, но ответ пока не получен, поэтому запись находится в «ожидании» и ещё не считается корректной.

Задание № 7

Условие:

Маршрутизатор блокирует исходящие подключения к DNS. Требуется разрешить хосту 10.10.10.1 отправлять DNS-запросы на корпоративный DNS-сервер 200.200.200.254. Выберите корректную команду iptables:

Ответ:

iptables -A OUTPUT -s 10.10.10.1 -d 200.200.200.254 -p udp --dport 53 -j ACCEPT

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

Решение:

Правило в цепочке OUTPUT с источником 10.10.10.1, назначением 200.200.200.254, протоколом UDP и портом назначения 53 разрешает именно исходящие DNS-запросы с нужного хоста к нужному серверу.

Задание № 8

Условие:
Какие функции выполняет технология reverse proxy?

Ответ:
- ○ Автоматически шифрует TCP/UDP-трафик (без предварительной конфигурации)
- ✓ Защищает BACKEND-серверы путём скрытия внутренней архитектуры
- ✓ Кэширует контент (статические данные, HTML и API)
- ✓ Поддерживает механизм балансировки нагрузки между нодами

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

Решение:
Reverse-прокси прячет внутренние backend-серверы, может кэшировать статический контент и распределять нагрузку между несколькими серверами, но не «шифрует всё автоматически» без настройки.

Задание № 9

Условие:

Какой протокол часто реализует отдельный процесс шифрования поверх L2TP для обеспечения криптографической защиты передаваемых данных?

Ответ:

- ○ OpenVPN
- ✓ IPSec
- ○ WireGuard
- ○ VLESS

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

Решение:

Классическая схема VPN «L2TP/IPSec» как раз использует L2TP только для туннелирования, а шифрование и аутентификацию целиком берёт на себя IPSec. Остальные протоколы либо сами уже включают шифрование (OpenVPN, WireGuard), либо вообще не используются как стандартный слой шифрования поверх L2TP.

Задание № 10

Условие:

Установите соответствие между протоколами туннелирования и их характеристиками.

Ответ:

L2TP	Канальный уровень, требует дополнительного шифрования, выполняет двойную инкапсуляцию
WireGuard	Прикладной уровень, использует современные криптографические алгоритмы, например, ChaCha20
IPsec	Сетевой уровень, два режима работы (транспортный и туннельный), реализует комплексную защиту
OpenVPN	Прикладной уровень, в основном для защиты сетевых соединений применяется TLS/SSL

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

Решение:

Протоколы туннелирования и характеристики
IPsec (1→a) работает на сетевом уровне и имеет транспортный и туннельный режимы; L2TP (2→b) — протокол канального уровня, обычно без встроенного шифрования; OpenVPN (3→c) использует TLS/SSL на прикладном уровне; WireGuard (4→d) — современный VPN с лёгкой криптографией (ChaCha20 и др.).

Задание № 11

Условие:

Как называется клиент-серверный протокол, обеспечивающий удалённое управление сетевыми устройствами в режиме CLI, но при этом **НЕ** шифрующий передаваемые данные в установленной сессии?

Ответ:

- ✓ Telnet
- ○ RDP
- ○ VNC
- ○ SSH

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

Решение:

Telnet предоставляет текстовый CLI-доступ, но не шифрует сессию, поэтому любые передаваемые данные можно перехватить в сети.

Задание № 12

Условие:
Что происходит при коллизии хэш-функции?

Ответ:
- ○ Нельзя восстановить исходный текст из хэша
- ✓ Хэш от двух разных текстов совпадает
- ○ Хэш от двух разных текстов различается
- ○ Любое изменение текста сильно меняет его хэш
- ○ Текст позволяет легко вычислить его хэш

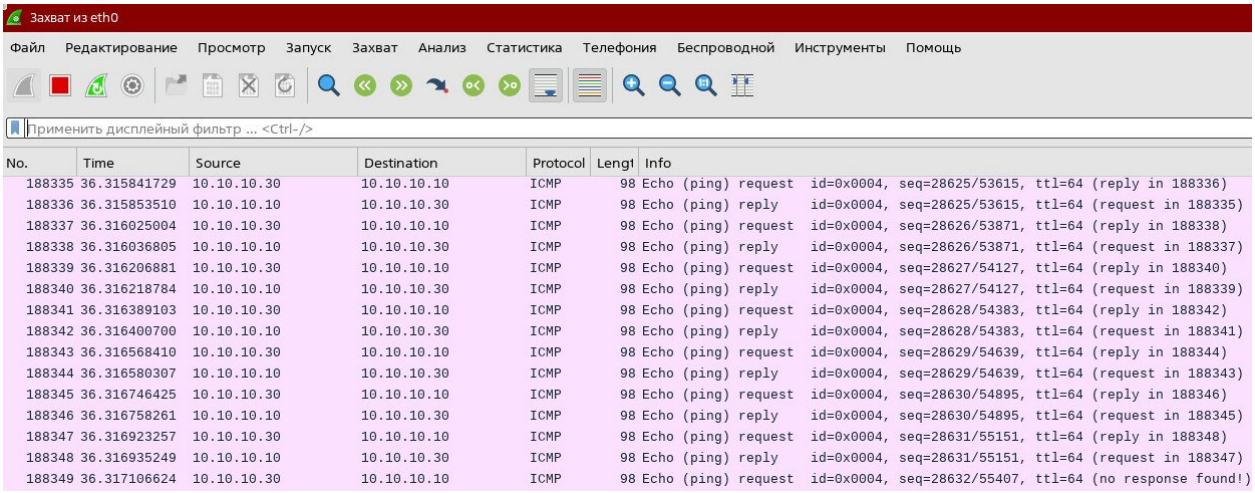
Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Решение:
Коллизия — это ситуация, когда два разных входных сообщения дают одинаковое хеш-значение, что нежелательно, но теоретически неизбежно для фиксированной длины хеша.

Задание № 13

Условие:

Какая атака приведёт к подобному результату?



Ответ:

- ○ IP Fragment Overlap
- ○ Teardrop Attack
- ✓ Ping Flood
- ○ ICMP Redirect Attack

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

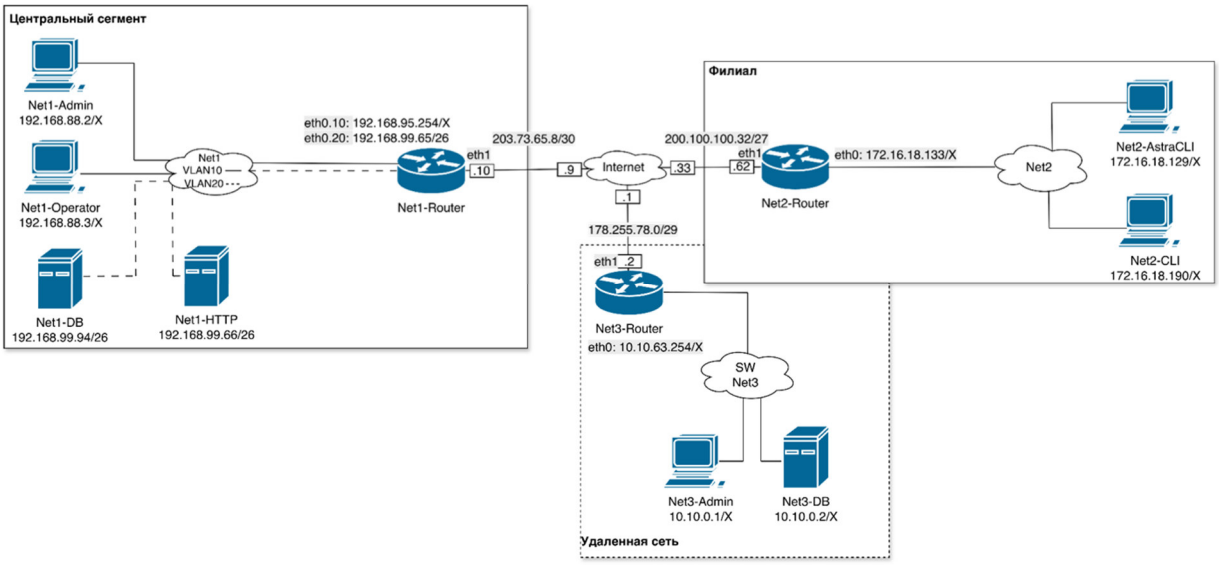
Решение:

На дампе видно, что на сервер-жертву .30 приходит большое количество ICMP Echo-Request пакетов с одного источника, что ведет необходимости ответа на каждый пакет и падению производительности сервера и занятию полосы пропускания. Такая атака называется Ping Flood. ICMP Redirect использует другой тип ICMP пакета (собственно, ICMP Redirect)

Задание № 14

Условие:

Дана схема сети.



К какой сети относятся Net1-Admin 192.168.88.2 и Net1-Operator 192.168.88.3, если известно, что префикс подсети — 20?

Ответ:

- ✓ 192.168.80.0/20
- ○ 192.168.88.0/24
- ○ 192.168.88.0/20
- ○ 192.168.0.0/16

Точное совпадение ответа — 1 балл

Решение:

При маске /20 шаг по третьему октету равен 16, поэтому диапазон 192.168.80.0–192.168.95.255 образует одну сеть, и адреса .88.x в неё попадают.

Условие:

Какой адрес является BROADCAST для WAN-сегмента Net1-Router?

Ответ:

- ○ 203.73.65.8
- ○ 203.73.65.9
- ○ 203.73.65.10
- ✓ 203.73.65.11

Точное совпадение ответа — 1 балл

Решение:
Если WAN-сегмент имеет подсеть вроде 203.73.65.8/30, то первый адрес — сетевой, два средних — хосты, а 203.73.65.11 — широковещательный, его и выбираем как BROADCAST.

Условие:
Какую максимальную длину префикса сети можно задать для подсети Net2, чтобы все её узлы оставались в одной подсети?

Ответ: 26
Точное совпадение ответа — 1 балл

Решение:
В Net2 достаточно адресов /26 (64 адреса, 62 рабочих), поэтому /26 — наибольший префикс, позволяющий разместить все указанные в схеме узлы.

Условие:
Нужно разрешить доступ к Net1-HTTP (192.168.99.66) из Интернета по протоколам HTTP и HTTPS. Какое правило iptables в цепи FORWARD нужно добавить на Net1 Router?

Ответ:
iptables -A FORWARD -i eth0 -p tcp -m multiport --dports 80, 443 -d 192.168.50.2 -j ACCEPT

За каждый выбранный ответ — 1 балл.

Решение:
-i eth0 обозначает внешний интерфейс, на который приходят запросы, а FORWARD — транзит к серверу. Поля -d 192.168.50.2 и --dports 80,443 вместе с -p tcp делают правило максимально точным: только HTTP/HTTPS к конкретному хосту.

Условие:
Какое правило используется для разрешения диагностики через ICMP на Net3-Router?

Ответ:
- ○ iptables -A FORWARD -p icmp -j ACCEPT
- ✓ iptables -A INPUT -p icmp -j ACCEPT
- ○ iptables -A OUTPUT -p icmp -j ACCEPT
- ○ iptables -P INPUT ACCEPT

Точное совпадение ответа — 1 балл

Решение:

Здесь нужна цепочка INPUT, потому что ICMP-эхо (ping) адресовано самому маршрутизатору, а не пересылается через него. Поле -p icmp выделяет только ICMP-пакеты, и -j ACCEPT разрешает их для диагностики.

Условие:
Необходимо разрешить перенаправление (маршрутизацию) трафика между подинтерфейсами Net1-Router. Какое правило IPTables нужно добавить?

Ответ:
iptables -A FORWARD -i eth0.10 -o eth0.20 -j ACCEPT

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.

Максимальный балл за задание — 12

Задание № 15

Условие:
Рекомендуемые утилиты: Python
Файл: reverse_9_3.cpp
Товарищ, секретный протокол коммуникации хакеров закодирован с помощью сложной комбинации операций. Нужно проследить каждое преобразование и вернуть оригинальное сообщение, иначе все данные будут потеряны. Восстановите исходный текст.
Шифротекст:
encoded =[99, 87, 69, 99, 48, 105, 126, 117, 75, 151, 154, 102, 3, 132, 109, 54, 154, 90, 105, 163, 3, 181, 118, 39, 66, 129]

Ответ: vsosh{lin34r_r3v3rs3_74sk}
Точное совпадение ответа — 3 балла
Максимальный балл за задание — 3

Решение:
1. XOR с ключом `{2, 3, 5, 7, 11, 13, 17, 19}`.
2. Линейное преобразование: `(val * 3 + 7) % 256`.
Для решения: находим обратное число для 3 по модулю 256 (это 171), вычисляем `(val - 7) * 171 % 256` и делаем XOR с ключом.
Ответ: `vsosh{lin34r_r3v3rs3_74sk}`
Пример решения на Python:

```
encoded = [...]
key = [2, 3, 5, 7, 11, 13, 17, 19]
res = ""
for i, val in enumerate(encoded):
    char_xor = (val - 7) * 171 % 256
    res += chr(char_xor ^ key[i % 8])
print(res)
```

Задание № 16

Условие:
Рекомендуемые утилиты: Wireshark
Файл: traffic_9_3.pcap
Товарищ, в наших информационных сетях обнаружена аномалия. Похоже, кто-то пытается получить несанкционированный доступ к файлам на сервере. Требуется срочное расследование и анализ ситуации.
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: 10.0.3.25
Точное совпадение ответа — 1 балл

Условие:
Какой файл был успешно прочитан злоумышленником?

Ответ: /etc/passwd

Точное совпадение ответа — 1 балл

Условие:
Определите переданный флаг.

Ответ: vsosh{p4th_tr4v3rs4l_lf1}

Точное совпадение ответа — 3 балла

Максимальный балл за задание — 6

Решение:
1/1/2/2 = 6
В HTTP-запросах видны попытки выхода за пределы директории (`../../etc/passwd`). Успешный запрос позволяет прочитать файл.
Целевые пакеты: 32, 34.
1. Тип атаки: Directory Traversal (LFI/RFI)
2. IP атакующего: 10.0.3.25
3. Прочитанный файл: /etc/passwd
4. Флаг: vsosh{p4th_tr4v3rs4l_lf1}

Задание № 17

Условие:

Рекомендуемые утилиты: Python, CyberChef

Файл: decode_9_3

Робот-курьер «Коммунар» доставил закодированное послание из центрального узла. Данные закодированы в базовом 32-байтном формате для передачи через старые системы связи, причём похоже, что закодированы не один раз. Ваша задача — извлечь секретную информацию.

Ответ: vsosh{b4s3_32_c0ur13r_m3ss4g3}

Точное совпадение ответа — 3 балл

Максимальный балл за задание — 3

Решение:

Многократное (11 раз) кодирование Base32. Отличается от Base64 используемым алфавитом (только заглавные буквы и цифры 2-7).

Ответ: `vsosh{b4s3_32_c0ur13r_m3ss4g3}`

Пример решения на Python:

```
import base64
data = "..."
for _ in range(11):
    data = base64.b32decode(data)
print(data)
```

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

