ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ИНФОРМАТИКА. ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
2025–2026 УЧ. Г. ШКОЛЬНЫЙ ЭТАП. 10–11 КЛАССЫ

**Максимальный балл за работу – 105.**

**Вводный инструктаж**

Товарищ стажёр! Добро пожаловать в мир науки и торжества человеческого разума! Вы проходите стажировку в отделе информационной безопасности Предприятия 3826 — сети научно-производственных комплексов, занимающихся созданием новейших технологий под руководством лучших умов нашей страны. Научные достижения Предприятия 3826 изменили жизнь не только наших соотечественников, но и жителей всего мира. К сожалению, есть люди, которые используют новейшие технологии во вред. Ваша задача — помочь команде Предприятия 3826 защитить комплекс от киберугроз и предотвратить восстание роботов, вызванное действиями злоумышленников.

**1.** Какие криптографические примитивы обеспечивают аутентификацию и целостность данных?

- HMAC (Hash-based Message Authentication Code)
- Digital Signature (цифровая подпись)
- Stream cipher (потоковый шифр)
- Message Authentication Code (MAC)
- Block cipher (блочный шифр)
- Hash function (хеш-функция)

**2.** Выберите верные утверждения о TLS.

- TLS использует только асимметричное шифрование
- TLS использует и асимметричное, и симметричное шифрование
- Сертификаты связывают открытый ключ с сущностью (именем)
- Самоподписанный сертификат всегда безопасен
- В TLS 1.3 удалён RSA key exchange
- SSLv3 — один из рекомендуемых стандартов

**3.** Какая команда Linux позволяет мониторить системные вызовы процесса в реальном времени?

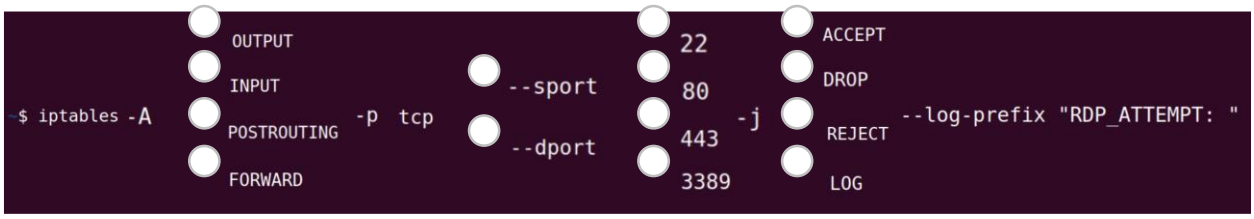
- strace
- ltrace
- gdb
- valgrind

**4.** Какой механизм в современных браузерах предотвращает выполнение JavaScript из недоверенных источников?

- Same-Origin Policy
- Content Security Policy
- CORS
- HSTS

**5.** Сколько байт занимает одно значение SHA-256 хэша?

**6.** В организации 3286 безопасники решили логировать все попытки подключения к охраняемой службе удалённого доступа рабочего стола администратора. Составьте подходящее правило.




**7.** Пистолет Макарова можно зарядить девятью патронами: 8 в обойму и 1 в патронник. Каждый патрон может быть с трассирующей пулей (X), бронебойной (Y) или обычной (Z).

Условия:

- для улучшения выцеливания обязательно должно быть ровно 3 патрона с трассером (X),
- патрон Y должен встречаться не менее одного раза,
- патрон Z может использоваться не более 2 раз, в том числе и не использоваться вовсе.

Сколько существует различных способов зарядить пистолет 9 патронами, соблюдая указанные условия? Одинаковые по составу раскладки, в которых позиции патронов отличаются, считаются различными.

## 8. Полимерный контейнер

Рекомендуемые утилиты: Python

Файл: decode_11_3

В лабораториях комплекса «Завод-3826» найден подозрительный файл с ключом к роботу-кодировщику. Исследователи подозревают, что данные закодированы каким-то необычным способом, возможно, кратность длины кодирования как-то с этим связана. Ваша задача — извлечь секретную информацию.

**Формат ответа: vsosh{...}**

## 9. Пассивный анализ

Рекомендуемые утилиты: python

Файл: reverse_11_3.py

Товарищ, на конвейере генератора ключей обнаружен сбой: каждый байт ключа сдвинули по позиции, «покрутили» и замаскировали. Верните исходный порядок и укажите корректный ключ.

**Формат ответа: vsosh{...}**

## 10. Временная калькуляция

IT-директор Олег установил максимальный уровень защиты на сервер с критически важными данными, но потерял листок с записанным паролем. В документации системы безопасности указаны параметры парольной политики:

- длина пароля составляете 8 символов;
- разрешены буквы английского алфавита (26 символов, регистр только нижний), цифры, спецсимволы;
- все цифры от 0 до 9;
- спецсимволы — только астериск (*), плюс (+), знак процента (%), амперсанд (&), знак доллара ($), знак равенства (=).

Сколько времени максимально уйдёт на подбор у профессионального инструмента для восстановления паролей, работающего со скоростью 2000 паролей в секунду? Ответ выразите в секундах, арифметически округлите до целых.

## 11. Сетевая аномалия

Рекомендуемые утилиты: Wireshark

Файл: traffic_11_3.pcap

Товарищ, в наших информационных сетях обнаружена аномалия. Кажется, кто-то атакует внутренние сервисы. Требуется срочное расследование и анализ ситуации. Исследуйте запись трафика и опишите атаку.

Какой тип атаки был применён?

- 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)

Определите IP-адрес атакующего.

Какой файл пытались прочитать с сервера?

Имя папки без символов слэша (/):

Файл:

Определите переданный флаг.
**Формат ответа: vsosh{...}**

**Максимальный балл за работу – 105.**