ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

Бланк заданий *Муниципальный этап, 2022*

Всероссийская олимпиада школьников по технологии

профиль «Информационная безопасность»

Муниципальный этап

10-11 класс

Максимальная оценка – 100 баллов, в том числе:

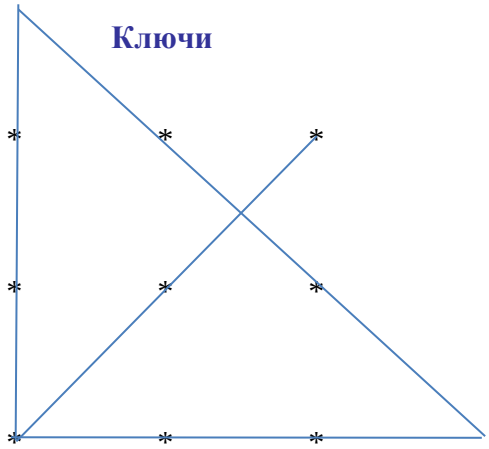
по 1 баллу за задания №№ 1-5

и

№ задания	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Балл	1	4	2	5	1	1	3	5	4	6	12	12	12	15	6	6

Ключи

Задание 1.



Задание 2.

Ответ: Г) нормы затрат физической и нервной энергии работников, Е) нормы затрат рабочего времени и соотношение численности, Ж) нормы результатов труда

Задание 3. Ответ: 1 - _Д_ , 2 - _Б_ , 3 - _А_ , 4 - _В_, 5 - _Г_.

Задание 4. Ответ: А) 3

Задание 5. Ответ: _90 тыс. руб._

Решение: Находим общую сумму доходов после уплаты НДФЛ в размере 134 тыс. 482 руб. 76 коп.

134 482, 76 * 87 / 13 = 900 000,009 руб. (округляем 900 тыс. руб. 00 коп.)

Находим сумму ежемесячных выплат по кредиту в размере 20% от суммы доходов семьи

900 000 *20 / 100 = 15 000 руб.

Находим общую сумму выплат по кредиту за полгода: 15 000 * 6 = 90 000 руб.

Задание 6. (1 балл) 272

Задание 7. (4 балла, по 1 баллу за каждые 2 этапа на своём месте) GDBACEF

Задание 8. (2 балла) c

Задание 9. (5 балла) 128

Задание 10. (1 балл) Нет

Задание 11. (1 балл) a

Задание 12. (3 балла, баллы начисляются только если ответ полностью совпадает) ab

Задание 13. (5 баллов) RIGHTANSWER

Задание 14. (4 балла) /etc/shadow

Задание 15. (До 6 баллов) За каждый способ защиты по 2 балла (максимум 3 способа):

1) Запрет аутентификации по паролю
2) Смена порта SSH
3) Запрет на вход под учётной записью администратора
4) Настройка сервисов против перебора (fail2ban)
5) Настройка IPS (Intrusion Prevention System)

Задание 16. (До 12 баллов) За каждый способ защиты по 4 балла (максимум 3 способа):

1) Настройка WAF (Web Application Firewall)
2) Настройка IPS/IDS
3) Изоляция веб-приложения (контейнер, виртуальная машина)
4) Настройка минимальных разрешения для сервисного пользователя веб-сервера (nginx, apache2)
5) Мониторинг состояния приложения и сервера

Задание 17. (До 12 баллов). За правильно определённую уязвимость – XSS (Межсайтовый скриптинг, Cross Site Scripting), 6 баллов. За описание способа защиты – 6 баллов.

Задание 18. (До 12 баллов). За правильное описание принципа эксплуатации – 12 баллов

Атака на уязвимость переполнения буфера на стеке заключается в перезаписи адреса возврата или других критичных элементов, расположенных на стеке. Таким образом, перезаписав адрес возврата, можно перенаправить поток выполнения программы в любом русле, например вызвать функцию system или execve для выполнения произвольных команд.

Задание 19. (До 15 баллов). За правильное описание принципа атаки – 6 баллов. За описание метода защиты – 9 баллов.

ARP-spoofing – разновидность атаки Man-in-the-Middle, применяемая в сетях с использованием протокола ARP. Данная атака выполняется следующим образом:

1. Злоумышленник отправляет два ARP-ответа (без запроса) – по одному пакету на каждое устройство между которыми будет осуществляться перехват пакетов.
2. Так как компьютеры поддерживают произвольный ARP, то после получения ARP-ответа, они изменят свои таблицы.
3. Теперь при отправке пакетов между этими компьютерами, данные будут проходить через устройство злоумышленника.

Способы защиты (засчитывается любой):

a) Программы отслеживания ARP-активности
b) VLAN
c) Статический ARP
d) Использование шифрования

Задание 20. (До 6 баллов). В зависимости от описанного способа начисляется разное количество баллов.

a) Хранение паролей “plain text”, в сыром виде – 1 балл
b) Хранение паролей с использованием симметричного шифрования (DES) – 2 балла
c) Хранение паролей с использованием симметричного шифрования (AES, 3DES, Кузнечик, Магма) – 3 балла
d) Хранение паролей с использованием ассиметричного шифрования (RSA, ГОСТ Р 34.10-2001) – 4 балла
e) Хранение паролей с использованием хэширования (MD4, MD5) – 5 баллов
f) Хранение паролей с использованием хэширования и соли (bcrypt, argon2) – 6 баллов

Задание 21. (До 6 баллов). За правильное описание уязвимости – 6 баллов.

Уязвимость format string возникает в случае передачи пользовательского ввода как первый аргумент для функций семейства printf(). Используя различные форматы вывода, атакующий способен читать и перезаписывать память программы.