Максимальное количество баллов за олимпиаду — 60

Задание 1. Вариант 1.

Тайное слово

Расследуя компьютерный инцидент, эксперт заметил, что в одном из файлов содержится закодированное слово — предположительно, это пароль.

10_2, 14_8, 1_{10}, 3_{16}, 1011_2, 23_8, 5_{10}, 1_{16}.

Едва взглянув на запись, он сообразил, что один из самых простых способов закодировать текст — это заменить каждую букву её порядковым номером в английском алфавите: A = 1, B = 2, C = 3 и т. д. Но что это за числа, записанные в виде нижних индексов рядом с номерами? Похоже, это основания систем счисления, в которые переведены их десятичные номера. Тогда, чтобы прочесть пароль, нужно перевести имеющиеся значения в десятичную систему счисления, а затем восстановить буквы по их кодам. Сделайте это и восстановите пароль.

Ответ: BLACKSEA

Критерий оценивания: точное совпадение ответа — 8 баллов

Максимальный балл за задание — 8

Решение.

Переведём числа из указанных систем счисления в десятичную и заменим порядковые номера буквами английского алфавита:

№	Значение	Система	Перевод в десятичную	Буква
1	10	2	2	B
2	14	8	12	L
3	1	10	1	A
4	3	16	3	C
5	1011	2	11	K
6	23	8	19	S
7	5	10	5	E
8	1	16	1	A

Ответ: BLACKSEA.

Задание 1. Вариант 2.

Тайное слово

Расследуя компьютерный инцидент, эксперт заметил, что в одном из файлов содержится закодированное слово — предположительно, это пароль.

6_{16}, 9_{10}, 12_{16}, 5_8, 10111_2, 1_{10}, 1100_2, 14_8.

Едва взглянув на запись, он сообразил, что один из самых простых способов закодировать текст — это заменить каждую букву её порядковым номером в английском алфавите: A = 1, B = 2, C = 3 и т. д. Но что это за числа, записанные в виде нижних индексов рядом с номерами? Похоже, это основания систем счисления, в которые переведены их десятичные номера. Тогда, чтобы прочесть пароль, нужно перевести имеющиеся значения в десятичную систему счисления, а затем восстановить буквы по их кодам. Сделайте это и восстановите пароль.

Ответ: FIREWALL

Критерий оценивания: точное совпадение ответа — 8 баллов

Максимальный балл за задание — 8

Решение по аналогии с вариантом 1

Задание 1. Вариант 3.

Тайное слово

Расследуя компьютерный инцидент, эксперт заметил, что в одном из файлов содержится закодированное слово — предположительно, это пароль.

20_8, 1_{10}, 23_8, 10011_2, 17_{16}, 15_{10}, 10010_2, 4_{16}.

Едва взглянув на запись, он сообразил, что один из самых простых способов закодировать текст — это заменить каждую букву её порядковым номером в английском алфавите: A = 1, B = 2, C = 3 и т. д. Но что это за числа, записанные в виде нижних индексов рядом с номерами? Похоже, это основания систем счисления, в которые переведены их десятичные номера. Тогда, чтобы прочесть пароль, нужно перевести имеющиеся значения в десятичную систему счисления, а затем восстановить буквы по их кодам. Сделайте это и восстановите пароль.

Ответ: PASSWORD

Критерий оценивания: точное совпадение ответа — 8 баллов

Максимальный балл за задание — 8

Решение по аналогии с вариантом 1

Задание 1. Вариант 4.

Тайное слово

Расследуя компьютерный инцидент, эксперт заметил, что в одном из файлов содержится закодированное слово — предположительно, это пароль.

5_{10}, 1110_2, 3_{10}, 12_{16}, 31_8, 10_{16}, 10100_2, 23_8.

Едва взглянув на запись, он сообразил, что один из самых простых способов закодировать текст — это заменить каждую букву её порядковым номером в английском алфавите: A = 1, B = 2, C = 3 и т. д. Но что это за числа, записанные в виде нижних индексов рядом с номерами? Похоже, это основания систем счисления, в которые переведены их десятичные номера. Тогда, чтобы прочесть пароль, нужно перевести имеющиеся значения в десятичную систему счисления, а затем восстановить буквы по их кодам. Сделайте это и восстановите пароль.

Ответ: ENCRYPTS

Критерий оценивания: точное совпадение ответа — 8 баллов

Максимальный балл за задание — 8

Решение по аналогии с вариантом 1

Задание 1. Вариант 5.

Тайное слово

Расследуя компьютерный инцидент, эксперт заметил, что в одном из файлов содержится закодированное слово — предположительно, это пароль.

10011_2, 5_{10}, 3_{16}, 21_{10}, 22_8, 1001_2, 24_8, 19_{16}.

Едва взглянув на запись, он сообразил, что один из самых простых способов закодировать текст — это заменить каждую букву её порядковым номером в английском алфавите: A = 1, B = 2, C = 3 и т. д. Но что это за числа, записанные в виде нижних индексов рядом с номерами? Похоже, это основания систем счисления, в которые переведены их десятичные номера. Тогда, чтобы прочесть пароль, нужно перевести имеющиеся значения в десятичную систему счисления, а затем восстановить буквы по их кодам. Сделайте это и восстановите пароль.

Ответ: SECURITY

Критерий оценивания: точное совпадение ответа — 8 баллов

Максимальный балл за задание — 8

Решение по аналогии с вариантом 1

Задание 1. Вариант 6.

Тайное слово

Расследуя компьютерный инцидент, эксперт заметил, что в одном из файлов содержится закодированное слово — предположительно, это пароль.

10_{16}, 10010_2, 17_8, 14_{16}, 1111_2, 3_{10}, 17_8, 12_{10}.

Едва взглянув на запись, он сообразил, что один из самых простых способов закодировать текст — это заменить каждую букву её порядковым номером в английском алфавите: A = 1, B = 2, C = 3 и т. д. Но что это за числа, записанные в виде нижних индексов рядом с номерами? Похоже, это основания систем счисления, в которые переведены их десятичные номера. Тогда, чтобы прочесть пароль, нужно перевести имеющиеся значения в десятичную систему счисления, а затем восстановить буквы по их кодам. Сделайте это и восстановите пароль.

Ответ: PROTOCOL

Критерий оценивания: точное совпадение ответа — 8 баллов

Максимальный балл за задание — 8

Решение по аналогии с вариантом 1

Задание 2.

Проверка пароля

Начинающий программист написал функцию, которая должна проверять, является ли пароль «надёжным». Пароль считается надёжным, если он соответствует всем условиям:

- длина не менее 8 символов;
- содержит хотя бы одну цифру;
- содержит хотя бы одну заглавную букву.

Функция, которую предоставил программист:

```
1  def is_strong_password(password):
2      length_ok = len(password) >= 8
3      has_digit = any(ch.isdigit() for ch in password)
4      has_upper = any(ch.isupper() for ch in password)
5      if length_ok or has_digit or has_upper:
6          return True
7      else:
8          return False
9
10 is_strong_password(password)
```

Проверьте, корректно ли работает программа на следующих паролях:

- `"abcdefgh"`
- `"Ab1"`

Определите статус этих паролей в логике, описанной в условии, а также результаты работы программы:

Пароль	**Соответствует критериям?**	**Результат работы программы**
`"abcdefgh"`	Да / Нет	`True` / `False`
`"Ab1"`	Да / Нет	`True` / `False`

Если в программе имеется ошибка, выберите номер строки, отвечающей за возникновение ошибки. Если ошибок нет, выберите строку 0.

Ответ:

Пароль	**Соответствует критериям?**	**Результат работы программы**
`"abcdefgh"`	Нет	`True`
`"Ab1"`	Нет	`True`

Номер строки: 5.

Критерий оценивания: точное совпадение ответа — 8 баллов

Максимальный балл за задание — 8

Решение.

Для пароля `"abcdefgh"`: `length_ok=True`, `has_digit=False`, `has_upper=False`. Так как используется `or`, результат `True`, то программа считает пароль надёжным, хотя на самом деле он ненадёжный: в нём нет цифр и заглавных букв.

Для пароля `"Ab1"`: `length_ok=False`, `has_digit=True`, `has_upper=True`. Из-за `or` результат тоже `True`, хотя пароль слишком короткий и ненадёжный.

Ошибка в строке

```
if length_ok or has_digit or has_upper:
```

Используется логическое ИЛИ (`or`) вместо И (`and`). Из-за этого достаточно выполнения любого одного условия, чтобы пароль был признан надёжным. Номер строки — 5.

Задание 3. Вариант 1.

Рекомендуемые инструменты: CyberChef, текстовый редактор

Файл: `03_audit.log`

Саша запускает текстовый редактор Mousepad, чтобы открыть файлы на компьютере secret-server (ОС Linux), используя специальный загрузчик, чтобы подменить имя процесса при запуске.

В файле `03_audit.log` сохранились события запуска процессов, которые записывает AuditD — системная служба аудита в ОС Linux.

Найдите флаг в формате `vsosh{xxxxxxxx}` в модифицированном названии запущенного процесса. Строка «xxxxxxxx» состоит из цифр и латинских букв в нижнем регистре.

Подсказка: обратите внимание на записи типа SYSCALL, EXECVE и PROCTITLE. В некоторых случаях данные закодированы. AuditD записывает некоторые значения в HEX-кодировке, если они содержат символы, которые так или иначе нарушают формат логов.

Ответ: `vsosh{good2bad}`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение.

В логе AuditD в событиях запуска процесса (syscall 59) есть несколько полей, где хранится информация о выполненной команде и исполняемом файле. Команда содержится в поле `proctitle` записи `type=PROCTITLE`, в полях `a0`, `a1` и т. д. записи `type=EXECVE`, а также в поле `comm` записи `type=SYSCALL`. Исполняемый файл указан в поле `comm` записи `type=SYSCALL` и поле `name` одной из записей `type=PATH`.

Из условия известно, что был запущен Mousepad (`/usr/bin/mousepad`), но с изменённым заголовком процесса. Поэтому нужно искать события, в которых исполняемый файл указан как `/usr/bin/mousepad`, а команда, прежде всего `proctitle`, отличается.

В файле `03_audit.log` находим события по строке `exe="/usr/bin/mousepad"`: их всего три. Уникальных значений поля `proctitle` два:

- `proctitle=666C61672076736F73687B676F6F64326261647D` (встречается дважды);
- `proctitle="xfce4-panel"`.

Первое значение закодировано в HEX. Декодирование даёт строку `flag vsosh{good2bad}`.

Альтернативный путь. Можно проверить все 15 записей `type=PROCTITLE`. Шесть указаны в явном виде и не содержат флага. Остаются девять записей (шесть уникальных), закодированных в HEX. Их декодирование даёт:

- `lightdm -session-child 15 29`;
- `/bin/bash /etc/lightdm/Xsession default`;
- `/usr/bin/xfce4-mime-helper -launch TerminalEmulator`;
- `tput setaf 1`;
- `dircolors -b`;
- `flag vsosh{good2bad}`.

Задание 3. Вариант 2.

Рекомендуемые инструменты: CyberChef, текстовый редактор

Файл: `03_audit.log`

Саша запускает текстовый редактор Mousepad, чтобы открыть файлы на компьютере secret-server (ОС Linux), используя специальный загрузчик, чтобы подменить имя процесса при запуске.

В файле `03_audit.log` сохранились события запуска процессов, которые записывает AuditD — системная служба аудита в ОС Linux.

Найдите флаг в формате `vsosh{xxxxxxxx}` в модифицированном названии запущенного процесса. Строка «xxxxxxxx» состоит из цифр и латинских букв в нижнем регистре.

Подсказка: обратите внимание на записи типа SYSCALL, EXECVE и PROCTITLE. В некоторых случаях данные закодированы. AuditD записывает некоторые значения в HEX-кодировке, если они содержат символы, которые так или иначе нарушают формат логов.

Ответ: `vsosh{time2win}`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение по аналогии с вариантом 1

Задание 3. Вариант 3.

Рекомендуемые инструменты: CyberChef, текстовый редактор

Файл: `03_audit.log`

Саша запускает текстовый редактор Mousepad, чтобы открыть файлы на компьютере secret-server (ОС Linux), используя специальный загрузчик, чтобы подменить имя процесса при запуске.

В файле `03_audit.log` сохранились события запуска процессов, которые записывает AuditD — системная служба аудита в ОС Linux.

Найдите флаг в формате `vsosh{xxxxxxxx}` в модифицированном названии запущенного процесса. Строка «xxxxxxxx» состоит из цифр и латинских букв в нижнем регистре.

Подсказка: обратите внимание на записи типа SYSCALL, EXECVE и PROCTITLE. В некоторых случаях данные закодированы. AuditD записывает некоторые значения в HEX-кодировке, если они содержат символы, которые так или иначе нарушают формат логов.

Ответ: `vsosh{inline64}`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение по аналогии с вариантом 1

Задание 3. Вариант 4.

Рекомендуемые инструменты: CyberChef, текстовый редактор

Файл: `03_audit.log`

Саша запускает текстовый редактор Mousepad, чтобы открыть файлы на компьютере secret-server (ОС Linux), используя специальный загрузчик, чтобы подменить имя процесса при запуске.

В файле `03_audit.log` сохранились события запуска процессов, которые записывает AuditD — системная служба аудита в ОС Linux.

Найдите флаг в формате `vsosh{xxxxxxxx}` в модифицированном названии запущенного процесса. Строка «xxxxxxxx» состоит из цифр и латинских букв в нижнем регистре.

Подсказка: обратите внимание на записи типа SYSCALL, EXECVE и PROCTITLE. В некоторых случаях данные закодированы. AuditD записывает некоторые значения в HEX-кодировке, если они содержат символы, которые так или иначе нарушают формат логов.

Ответ: `vsosh{lucky13s}`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение по аналогии с вариантом 1

Задание 3. Вариант 5.

Рекомендуемые инструменты: CyberChef, текстовый редактор

Файл: `03_audit.log`

Саша запускает текстовый редактор Mousepad, чтобы открыть файлы на компьютере secret-server (ОС Linux), используя специальный загрузчик, чтобы подменить имя процесса при запуске.

В файле `03_audit.log` сохранились события запуска процессов, которые записывает AuditD — системная служба аудита в ОС Linux.

Найдите флаг в формате `vsosh{xxxxxxxx}` в модифицированном названии запущенного процесса. Строка «xxxxxxxx» состоит из цифр и латинских букв в нижнем регистре.

Подсказка: обратите внимание на записи типа SYSCALL, EXECVE и PROCTITLE. В некоторых случаях данные закодированы. AuditD записывает некоторые значения в HEX-кодировке, если они содержат символы, которые так или иначе нарушают формат логов.

Ответ: `vsosh{version0}`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение по аналогии с вариантом 1

Задание 4. Вариант 1.

Файл: `index.html`

В исследовательском центре профессора Бита произошёл инцидент: один из сотрудников смог получить доступ к документу, который не предназначался для его учётной записи.

Специалисты по информационной безопасности сохранили копию веб-системы центра и попросили вас проверить, как работает просмотр документов.

После открытия сайта вы увидите личный кабинет сотрудника и список доступных ему документов:

- документ № 201;
- документ № 202;
- документ № 203.

Разработчик системы утверждает, что пользователь может просматривать только документы, которые отображаются в его личном кабинете.

Проверьте, действительно ли это так.

Найдите документ, который не отображается в списке доступных, но всё равно открывается через систему.

Внутри него находится код подтверждения. Запишите его без пробелов.

Ответ: `BIT-1A422466`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение.

В личном кабинете видны ссылки только на документы 201, 202 и 203.

Скрытый служебный документ имеет `id=206`. В адресной строке нужно указать `index.html?id=206`. В этом документе находится код подтверждения `BIT-1A422466`.

Задание 4. Вариант 2.

Файл: `index.html`

В исследовательском центре профессора Бита произошёл инцидент: один из сотрудников смог получить доступ к документу, который не предназначался для его учётной записи.

Специалисты по информационной безопасности сохранили копию веб-системы центра и попросили вас проверить, как работает просмотр документов.

После открытия сайта вы увидите личный кабинет сотрудника и список доступных ему документов:

- документ № 201;
- документ № 202;

- документ № 203.

Разработчик системы утверждает, что пользователь может просматривать только документы, которые отображаются в его личном кабинете.

Проверьте, действительно ли это так.

Найдите документ, который не отображается в списке доступных, но всё равно открывается через систему.

Внутри него находится код подтверждения. Запишите его без пробелов.

Ответ: `BIT-AD1F34F5`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение по аналогии с вариантом 1

Задание 4. Вариант 3.

Файл: `index.html`

В исследовательском центре профессора Бита произошёл инцидент: один из сотрудников смог получить доступ к документу, который не предназначался для его учётной записи.

Специалисты по информационной безопасности сохранили копию веб-системы центра и попросили вас проверить, как работает просмотр документов.

После открытия сайта вы увидите личный кабинет сотрудника и список доступных ему документов:

- документ № 201;
- документ № 202;
- документ № 203.

Разработчик системы утверждает, что пользователь может просматривать только документы, которые отображаются в его личном кабинете.

Проверьте, действительно ли это так.

Найдите документ, который не отображается в списке доступных, но всё равно открывается через систему.

Внутри него находится код подтверждения. Запишите его без пробелов.

Ответ: `BIT-AA1F303C`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение по аналогии с вариантом 1

Задание 4. Вариант 4.

Файл: `index.html`

В исследовательском центре профессора Бита произошёл инцидент: один из сотрудников смог получить доступ к документу, который не предназначался для его учётной записи.

Специалисты по информационной безопасности сохранили копию веб-системы центра и попросили вас проверить, как работает просмотр документов.

После открытия сайта вы увидите личный кабинет сотрудника и список доступных ему документов:

- документ № 201;
- документ № 202;
- документ № 203.

Разработчик системы утверждает, что пользователь может просматривать только документы, которые отображаются в его личном кабинете.

Проверьте, действительно ли это так.

Найдите документ, который не отображается в списке доступных, но всё равно открывается через систему.

Внутри него находится код подтверждения. Запишите его без пробелов.

Ответ: `BIT-AB1F31CF`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение по аналогии с вариантом 1

Задание 4. Вариант 5.

Файл: `index.html`

В исследовательском центре профессора Бита произошёл инцидент: один из сотрудников смог получить доступ к документу, который не предназначался для его учётной записи.

Специалисты по информационной безопасности сохранили копию веб-системы центра и попросили вас проверить, как работает просмотр документов.

После открытия сайта вы увидите личный кабинет сотрудника и список доступных ему документов:

- документ № 201;
- документ № 202;
- документ № 203.

Разработчик системы утверждает, что пользователь может просматривать только документы, которые отображаются в его личном кабинете.

Проверьте, действительно ли это так.

Найдите документ, который не отображается в списке доступных, но всё равно открывается через систему.

Внутри него находится код подтверждения. Запишите его без пробелов.

Ответ: `BIT-A81F2D16`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение по аналогии с вариантом 1

Задание 4. Вариант 6.

Файл: `index.html`

В исследовательском центре профессора Бита произошёл инцидент: один из сотрудников смог получить доступ к документу, который не предназначался для его учётной записи.

Специалисты по информационной безопасности сохранили копию веб-системы центра и попросили вас проверить, как работает просмотр документов.

После открытия сайта вы увидите личный кабинет сотрудника и список доступных ему документов:

- документ № 201;
- документ № 202;
- документ № 203.

Разработчик системы утверждает, что пользователь может просматривать только документы, которые отображаются в его личном кабинете.

Проверьте, действительно ли это так.

Найдите документ, который не отображается в списке доступных, но всё равно открывается через систему.

Внутри него находится код подтверждения. Запишите его без пробелов.

Ответ: `BIT-A91F2EA9`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение по аналогии с вариантом 1

Задание 5. Вариант 1.

Рекомендуемые инструменты: Wireshark

Файл: `challenge.pcap`

Продолжая расследование компьютерного инцидента, эксперт изучил запись сетевой активности устройств в локальной сети. Далее он заметил, что при посещении различных сайтов происходило обращение к DNS-серверам, один из которых подлинный, а второй — по-видимому, контролируется нарушителем. У системного администратора он узнал IP-адрес подлинного DNS-сервера: `172.30.0.10`.

Определите IP-адрес DNS-сервера, контролируемого нарушителями.

Ответ: `172.30.0.66`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение.

1. Отфильтровать DNS-трафик. Откроем файл `challenge.pcap` в Wireshark и введём в строку фильтра `dns`. После применения фильтра останутся DNS-запросы и DNS-ответы. Запросы можно узнать по тексту `Standard query` в колонке `Info`, ответы — по тексту `Standard query response`. Чтобы оставить только ответы, можно использовать фильтр `dns.flags.response == 1`.

2. Найти IP-адреса DNS-серверов. Просмотрим колонку `Source` у DNS-ответов. Большая часть ответов приходит от `172.30.0.10` — известного подлинного DNS-сервера. В коротком интервале встречаются ответы от другого адреса. Для первого варианта он равен `172.30.0.66`.

3. Проверить вывод. У одного ответа от второго адреса посмотрим `Transaction ID` в поле `Domain Name System`. Рядом есть ответ от `172.30.0.10` с тем же `Transaction ID`, но с другим IP-адресом в A-записи. Это подтверждает подмену DNS-ответа.

Адрес `172.30.0.99` находится внутри A-записи. Это адрес сайта, а не DNS-сервера. Ответом является значение из колонки `Source`.

Задание 5. Вариант 2.

Рекомендуемые инструменты: Wireshark

Файл: `challenge.pcap`

Продолжая расследование компьютерного инцидента, эксперт изучил запись сетевой активности устройств в локальной сети. Далее он заметил, что при посещении различных сайтов происходило обращение к DNS-серверам, один

из которых подлинный, а второй — по-видимому, контролируется нарушителем. У системного администратора он узнал IP-адрес подлинного DNS-сервера: `172.30.0.10`.

Определите IP-адрес DNS-сервера, контролируемого нарушителями.

Ответ: `172.30.0.61`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение по аналогии с вариантом 1

Задание 5. Вариант 3.

Рекомендуемые инструменты: Wireshark

Файл: `challenge.pcap`

Продолжая расследование компьютерного инцидента, экперт изучил запись сетевой активности устройств в локальной сети. Далее он заметил, что при посещении различных сайтов происходило обращение к DNS-серверам, один из которых подлинный, а второй — по-видимому, контролируется нарушителем. У системного администратора он узнал IP-адрес подлинного DNS-сервера: `172.30.0.10`.

Определите IP-адрес DNS-сервера, контролируемого нарушителями.

Ответ: `172.30.0.66`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение по аналогии с вариантом 1

Задание 5. Вариант 4.

Рекомендуемые инструменты: Wireshark

Файл: `challenge.pcap`

Продолжая расследование компьютерного инцидента, экперт изучил запись сетевой активности устройств в локальной сети. Далее он заметил, что при посещении различных сайтов происходило обращение к DNS-серверам, один из которых подлинный, а второй — по-видимому, контролируется нарушителем. У системного администратора он узнал IP-адрес подлинного DNS-сервера: `172.30.0.10`.

Определите IP-адрес DNS-сервера, контролируемого нарушителями.

Ответ: `172.30.0.71`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение по аналогии с вариантом 1

Задание 5. Вариант 5.

Рекомендуемые инструменты: Wireshark

Файл: `challenge.pcap`

Продолжая расследование компьютерного инцидента, экперт изучил запись сетевой активности устройств в локальной сети. Далее он заметил, что при посещении различных сайтов происходило обращение к DNS-серверам, один из которых подлинный, а второй — по-видимому, контролируется нарушителем. У системного администратора он узнал IP-адрес подлинного DNS-сервера: `172.30.0.10`.

Определите IP-адрес DNS-сервера, контролируемого нарушителями.

Ответ: `172.30.0.76`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение по аналогии с вариантом 1

Задание 5. Вариант 6.

Рекомендуемые инструменты: Wireshark

Файл: `challenge.pcap`

Продолжая расследование компьютерного инцидента, экперт изучил запись сетевой активности устройств в локальной сети. Далее он заметил, что при посещении различных сайтов происходило обращение к DNS-серверам, один из которых подлинный, а второй — по-видимому, контролируется нарушителем. У системного администратора он узнал IP-адрес подлинного DNS-сервера: `172.30.0.10`.

Определите IP-адрес DNS-сервера, контролируемого нарушителями.

Ответ: `172.30.0.81`

Критерий оценивания: точное совпадение ответа — 10 баллов

Максимальный балл за задание — 10

Решение по аналогии с вариантом 1

Задание 6. Вариант 1.

Файлы: `Crypto_windows.exe`, `Crypto_linux`

На компьютере одного из пользователей эксперт обнаружил программу, с помощью которой он зашифровывал свои пароли. Шифратор принимает только цифры и латинские буквы, заменяя заглавные буквы на строчные. Другие символы удаляются из строки.

Один из паролей в зашифрованном виде выглядит так: «kepyuoav». Восстановите исходный пароль и получите флаг в формате `vsosh{xxxxxxxx}`, где «xxxxxxxx» — пароль в открытом (незашифрованном) виде.

Подсказка: в вашем распоряжении имеются реализации программы-шифратора для ОС Windows и Linux. Количество попыток ввода текста не ограничено. Иногда, вводя разные значения открытого текста и наблюдая за шифртекстом, можно определить, какой шифр реализован.

Ответ: `vsosh{qwerty67}`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение.

Поскольку в задании указано, что программа шифрует пароли, можно исходить из того, что она реализует какой-то шифр. Основными операциями, применяемыми для построения шифров, являются замена и перестановка. Будем последовательно подавать на вход различные строки, анализировать выводы и делать выводы:

Входная строка	Выходная строка	Вывод
`abc`	`g3x`	Присутствует операция замены
`bac`	`3gx`	Перестановка, вероятно, отсутствует
`aaabbbccc`	`ggg333xxx`	Вероятно, реализована простая замена
`abcdefghijklm` `nopqrstuvwxyz`	`g3xcpmzfsi270` `j6nky9udhebol`	Получили таблицу замены для букв; символы «a» и «v» не обнаружены — вероятно, это цифры
`1234567890`	`8wt51avrq4`	Обнаружили, какие символы зашифровываются в «a» и «v»: это «6» и «7»
`qrstuvwxyz`	`ky9udhebol`	Ещё раз зашифровали часть алфавита, которая даёт основную часть интересующих символов замены
`qwerty67`	`kepyuoav`	Собрали открытый текст, соответствующий наблюдаемым буквам, чтобы получить требуемый шифртекст

Задание 6. Вариант 2.

Файлы: `Crypto_windows.exe`, `Crypto_linux`

На компьютере одного из пользователей эксперт обнаружил программу, с помощью которой он зашифровывал свои пароли. Шифратор принимает только цифры и латинские буквы, заменяя заглавные буквы на строчные. Другие символы удаляются из строки.

Один из паролей в зашифрованном виде выглядит так: «kbcrl8ft». Восстановите исходный пароль и получите флаг в формате `vsosh{xxxxxxxx}`, где «xxxxxxxx» — пароль в открытом (незашифрованном) виде.

Подсказка: в вашем распоряжении имеются реализации программы-шифратора для ОС Windows и Linux. Количество попыток ввода текста не ограничено. Иногда, вводя разные значения открытого текста и наблюдая за шифртекстом, можно определить, какой шифр реализован.

Ответ: `vsosh{univer26}`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение по аналогии с вариантом 1

Задание 6. Вариант 3.

Файлы: `Crypto_windows.exe`, `Crypto_linux`

На компьютере одного из пользователей эксперт обнаружил программу, с помощью которой он зашифровывал свои пароли. Шифратор принимает только цифры и латинские буквы, заменяя заглавные буквы на строчные. Другие символы удаляются из строки.

Один из паролей в зашифрованном виде выглядит так: «yk0co6wj». Восстановите исходный пароль и получите флаг в формате `vsosh{xxxxxxxx}`, где «xxxxxxxx» — пароль в открытом (незашифрованном) виде.

Подсказка: в вашем распоряжении имеются реализации программы-шифратора для ОС Windows и Linux. Количество попыток ввода текста не ограничено. Иногда, вводя разные значения открытого текста и наблюдая за шифртекстом, можно определить, какой шифр реализован.

Ответ: `vsosh{codez3r0}`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение по аналогии с вариантом 1

Задание 6. Вариант 4.

Файлы: `Crypto_windows.exe`, `Crypto_linux`

На компьютере одного из пользователей эксперт обнаружил программу, с помощью которой он зашифровывал свои пароли. Шифратор принимает только цифры и латинские буквы, заменяя заглавные буквы на строчные. Другие символы удаляются из строки.

Один из паролей в зашифрованном виде выглядит так: «xingajoy». Восстановите исходный пароль и получите флаг в формате `vsosh{xxxxxxxx}`, где «xxxxxxxx» — пароль в открытом (незашифрованном) виде.

Подсказка: в вашем распоряжении имеются реализации программы-шифратора для ОС Windows и Linux. Количество попыток ввода текста не ограничено. Иногда, вводя разные значения открытого текста и наблюдая за шифртекстом, можно определить, какой шифр реализован.

Ответ: `vsosh{zxspec82}`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение по аналогии с вариантом 1

Задание 6. Вариант 5.

Файлы: `Crypto_windows.exe`, `Crypto_linux`

На компьютере одного из пользователей эксперт обнаружил программу, с помощью которой он зашифровывал свои пароли. Шифратор принимает только цифры и латинские буквы, заменяя заглавные буквы на строчные. Другие символы удаляются из строки.

Один из паролей в зашифрованном виде выглядит так: «rx1utam9». Восстановите исходный пароль и получите флаг в формате `vsosh{xxxxxxxx}`, где «xxxxxxxx» — пароль в открытом (незашифрованном) виде.

Подсказка: в вашем распоряжении имеются реализации программы-шифратора для ОС Windows и Linux. Количество попыток ввода текста не ограничено. Иногда, вводя разные значения открытого текста и наблюдая за шифртекстом, можно определить, какой шифр реализован.

Ответ: `vsosh{intel486}`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение по аналогии с вариантом 1

Задание 6. Вариант 6.

Файлы: `Crypto_windows.exe`, `Crypto_linux`

На компьютере одного из пользователей эксперт обнаружил программу, с помощью которой он зашифровывал свои пароли. Шифратор принимает только цифры и латинские буквы, заменяя заглавные буквы на строчные. Другие символы удаляются из строки.

Один из паролей в зашифрованном виде выглядит так: «r0afhzxi». Восстановите исходный пароль и получите флаг в формате `vsosh{xxxxxxxx}`, где «xxxxxxxx» — пароль в открытом (незашифрованном) виде.

Подсказка: в вашем распоряжении имеются реализации программы-шифратора для ОС Windows и Linux. Количество попыток ввода текста не ограничено. Иногда, вводя разные значения открытого текста и наблюдая за шифртекстом, можно определить, какой шифр реализован.

Ответ: `vsosh{price402}`

Критерий оценивания: точное совпадение ответа — 12 баллов

Максимальный балл за задание — 12

Решение по аналогии с вариантом 1

