

Муниципальный этап ВСОШ по дисциплине Информационная безопасность.

Критерии оценки участников:

Муниципальный этап ВСОШ проводился по правилам CTF, где участники должны решать задания по направлениям информационной безопасности.

Для получения баллов за выполнение задания участник должен ввести в поля ответа «флаг». Формат флага был NMARK{ }.

Задания делятся на «очень простые», «простые», «средние» и «сложные».

За очень простые задания участнику начисляется 20 баллов, за простые 30 баллов, за средние 70 баллов, за сложные 100 баллов.

Побеждает тот кто первым наберет максимальное количество баллов.

Задания и баллы за них:

Безопасность web.

Бобровый домик

20 баллов

Бобры пригласили тебя в гости. В процессе чаепития они потеряли очень ценные 2 бревна. Помоги им найти брёвна.

Криптография.

Салат - Панкосвод

30 баллов

Котик! Я тут тебе готовила салат, пробовала различные ингредиенты, смешивала. Да что-то так намешала, что получилось очень вкусно. Но вот проблема - я не помню, что там было изначально. Помоги, пожалуйста, восстановить салат.

Флаг был зашифрован приложенным скриптом:

```
NMARK{zhml_rlf_buzhml_jpwoly_huk_h_jvyylja_mshn_dpao_dvykz_nv_zbiitpa}
```

В программе флаг был убран из кода, восстановите его из зашифрованных данных. В правильно расшифрованном флаге содержится слово correct.

Салат - Кризотютя

30 баллов

Котик! Я тебе на 8 марта приготовил подарок, но он как-то перемешался по дороге в пакете. Я не знаю, как его восстановить! Может, ты сможешь?

В результате шифрования приложенной программой получился следующий вывод:
ciphertext =

```
6653a882e12bba271dcf307092be3b2aa331e51edb777c8c8fd831a02b1bd13073cbec6  
514a26aa10f
```

hint = 6b7f87f0d33fbb6f10d90c6487af2855b436f90180

В программе флаг был убран из кода, восстановите его из зашифрованных данных.

Безопасность сети.

Бобры строят умную платину

30 баллов

Бобры платину начали строить, но датчиков всяких полно было, и начали искать протокол, который бы позволил с ними работать. Протокол то нашли, а вот среди него флаг потеряли.

Бобры сообразили

70 баллов

Бобры достроили плотину. Но нужно было мониторинг наладить. Сделали плотине веб-интерфейс в виде **Hyper** бобра. Бобер был глухонемой, поэтому только **Text** мог передавать. Чтобы бобёр, сидя на одном месте не утонул в грязи, ему **Trancfer-ом** привезли бревна для дома и сразу же за **3a-Protocol-ировали** новую постройку. Кстати, пока интербобру дом строили, посмотрели все протоколы (вы знали, что у бобров есть **!иерархия!?**), но поняли, что всего **1 протокол** для постановки на учёт нужен, да и бобёр любил английские словосочетания сокращать. Но на запросы **Requests**, которые, кстати, тем же протоколом отправляли, отвечал исправно, иногда тканевые картинки .png отправлял! Однажды бобра попросили флаг найти, чтобы над плотинкой бобровые знамя поднять, а бобер обжился по-тихоньку на роли зрителя платины и !фильтр! для воды себе поставил, да не простой, а программируемый, но староватый. И решил наш незатейливый герой из картинке флаг сделать, и начал объяснить фильтру, чтобы отмывать придётся картинку от букв отчёта. Он ввёл синтаксически всё верно, а на глючном интерфейсе показалось лишь `????r???est.uri == "/?L???2.?n?"`. В итоге отмыл он всё таки картинку, чтобы из неё флаг сделать, но рисовать - краски кончились, поэтому комментарии comments ! просто картинку зелёной травой измазал, а сверху черным маркером флаг написал. И теперь всяк, кто ! ИЗ ! разных сторон на **64-ю** плотину смотрел, видел её и *base* ! бобра-зрителя.

Безопасность операционных систем.

Иголка в стоге сена

30 баллов

Мы перехватили странный системный дамп `memory_dump.bin`. Внутри, кажется, есть флаг, но файл слишком огромный. Как-то нужно найти его.

Кот-сисадмин

70 баллов

Посмотрите лог `system_audit.log`. В 99% случаев там скучные записи о том, как запускается планировщик задач. Но в одной строке происходит какая-то дичь. Системный администратор клянётся, что в этот момент его кот прыгнул на клавиатуру и напечатал кучу непонятных символов. Но мы-то знаем, что коты не умеют пользоваться командой `sudo`... Или умеют? Переведите с "кошачьего" языка на человеческий и заберите флаг.

Реверс-инженерия

mini-bobry

70 баллов

Дорогой друг. Я спокойно шёл по лесу, собирал ягоды и грибы и вдруг встретил кое-что необычное. Это была семья мини-бобров. Они сказали, что не пропустят меня дальше, пока я не принесу им дерево. Да такое дерево, которое им понравится. Помоги мне узнать, какое дерево им нужно.

Вам помогут: `uncompress6` или `rusdc`

human reverse

100 баллов

Товарищ! Валерия Николаевна сконструировала робота-женщину-ревёрсера, которая поможет разревёрсить `Bombombini Gusini`. Она отправила тебе помощницу вместе с инструкцией. К сожалению, инструкция потерялась, а ревёрсить надо. А без активации не получится. Придётся тебе разревёсить и активировать помощницу. Для активации нужно отправить какие-то команды. Разберись, какие и в каком формате.

Вам помогут: `Ghidra`

Подробный разбор каждого задания будет выложен по адресу:
<https://github.com/mc-Daniil/municipal>