UGRACTF

Материалы заключительного этапа юниорской олимпиады по информационной безопасности Ugra CTF 2018–2019 гг.

Секретные архивы

Стеганография, 50 баллов

Как известно, в интернете ничего заблокировать нельзя: те, кому нужно, смогут найти способ передать секретные данные.
`ucucu.ga/19f/anonymous/public/dump.pcap`

Решение
В приведенном снимке сетевого трафика данные передаются по протоколу Gopher. В трафике можно найти архив и пароль от него.
`ucucu.ga/19f/anonymous/WRITEUP.md`

Ответ
`ugra_you_are_good_decryptor`

Данное устройство

Электроника, 500 баллов

С помощью данного устройства можно не только, но и!
`ucucu.ga/19f/apparatus/public/apparatus.jpg`
`ucucu.ga/19f/apparatus/public/apparatus.ino`
`ucucu.ga/19f/apparatus/public/apparatus.mp4`

Решение
По фотографии и программному коду узнаём соответствие кнопок и светодиодов. Просмотрев видео, записываем нажатые кнопки и получаем флаг, используя получившееся число.
`ucucu.ga/19f/apparatus/WRITEUP.md`

Ответ
`ugra_saratov_vladimir_penza_tula_taganrog_samara_omsk_kirov_tambov`

Огни большого города

Сетевая разведка, 350 баллов

Где находится балкон с таким замечательным видом?
`ucucu.ga/19f/bigcitylights/app/IMG_2223.jpg`
`https://bigcitylights.ugractf.ru`

Решение
Находим известные московские здания на фотографии. Соотнося их местоположение на фотографии и на карте, находим место съемки.
`ucucu.ga/19f/bigcitylights/WRITEUP.md`

Ответ
`ugra_come_to_Moscow_we_have_Sokol_and_Sokolniki_and_Sokolinaya_Gora`

Для слепых

Стеганография, 100 баллов

Даже слепой может читать между строк...
`ucucu.ga/19f/blind/public/task.pdf`

Решение
Флаг написан пиксельным шрифтом с размером символа 5×5 пикселей, каждый пиксель задавался одной страницей файла.
`ucucu.ga/19f/blind/WRITEUP.md`

Ответ
`ugra_preview`

Арбалеты Сибири

Реверс-инжиниринг, 450 баллов

Вы запустите.
`ssh game@ugractf.ru -p 5004`,
password `game`
`ucucu.ga/19f/bow/public/bow`

Решение
Дана скомпилированная компьютерная игра про стрельбу из лука. Необходимо разобраться в физической модели и подобрать правильные параметры.
`ucucu.ga/19f/bow/WRITEUP.md`

Ответ
`ugra_you_have_found_the_correct_vector`

Леденящее дыхание

Бонус, 100 баллов

И так всё понятно. Оригинал
`ucucu.ga/19f/exhale/public/trump.mp4`

Решение
Из видео с публичным обращением Дональда Трампа вырезали речь, оставив лишь склейки дыхания. Можно восстановить фрагменты, сопоставив кадры с оригинальным роликом. Флаг составляется из первых букв произносимых слов.
`ucucu.ga/19f/exhale/WRITEUP.md`

Ответ
`ugra_joshua_the_boi_with_his_rabbit_wife`

Битва экстрасенсов

Бинарная эксплуатация, 300 баллов

Иногда задачи бывают странные... Но на CTF-соревнованиях пригодятся все скиллы, в том числе и ясновидение. Поможет ли чекер угадать ответ с первой попытки? Флаг от этого задания будет доступен на странице «отчёт».
`contest.yandex.ru/contest/12894/problems/3`
`ucucu.ga/19f/extrasense/public/check`

Решение
В данном задании был дан чекер с уязвимостью выхода за пределы массива. Необходимо было её проэксплуатировать, сдав специально сформированный ответ.
`ucucu.ga/19f/extrasense/WRITEUP.md`

Ответ
`ugra_peter_pwner_is_guesser`

Инновационные технологии

Веб-технологии, 150 баллов

9 лет назад одна компания решила обезопасить своих пользователей и предоставить им доступ к своему сайту только по самым безопасным протоколам того времени.
Кто бы мог подумать, что сегодня почти никто и не сможет открыть их сайт...
`https://legacy-old.ugractf.ru/`

Решение
Необходимо было посетить сайт, доступный по протоколу SSLv3: он не работает в современных ОС и браузерах.
`ucucu.ga/19f/modern/WRITEUP.md`

Ответ
`ugra_2010_got_back_today`

noteasy³

Криптография, 200 баллов

[Изображение кубической параболы, вдоль которой написана фраза «Произошла криптография»]

Алфавит шифра:
`ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz_`
Подсказка: cherchez la fonction
`ucucu.ga/19f/noteasy3/public/flag.enc.txt`

Решение
Используется аффинный шифр вида $y = (ax^3 + bx^2 + cx + d) \bmod 53$, по четырём первым буквам флага подбирались коэффициенты.
`ucucu.ga/19f/noteasy3/WRITEUP.md`

Ответ
`ugra_eNcrYPt_DaTA_haRDer`

Сразу видно, олдскул

Форензика, 150 баллов

Помимо любителей анонимности, всякими специфичными протоколами пользуются просто ради забавы... Разумеется, все секреты хранятся общедоступно и никак не скрываются.
`files/anonymous/dump.pcap`

Решение
В снимке сетевого трафика можно обнаружить следы коммуникации по протоколу Gopher, повторить действия, совершённые жертвой и получить флаг.
`ucucu.ga/19f/olds/WRITEUP.md`

Ответ
`ugra_i_like_gopher_links`

В семь шуб одет

Стеганография, 350 баллов

Аппетит приходит во время еды, а метафоры раскрываются постепенно.
`ucucu.ga/19f/onionion/public/island-in-the-ocean.jpg`

Решение
Данная задача была составлена из семи простых уровней стеганографической защиты, нужно было снять их все.
`ucucu.ga/19f/onionion/WRITEUP.md`

Ответ
`ugra_will_you_make_the_villain_die_after_all`

OOOверфлоу

Бинарная эксплуатация, 200 баллов

Сотрудники одного московского ООО разработали уникальную систему защиты под названием SegFault™, которая срабатывает, когда кто-то пытается взломать их программы. Или нет.
nc ugractf.ru 5002
`ucucu.ga/19f/oooverflow/public/service`

Решение
При чтении строки отсутствуют какие-либо ограничения на размер ввода, что позволяет переполнить буфер и перезаписать адрес возврата.
`ucucu.ga/19f/oooverflow/WRITEUP.md`

Ответ
`ugra_pointer_tourist`

OOOверфлоу 2.0

Бинарная эксплуатация, 350 баллов

Сотрудники одного московского ООО учли свои ошибки. Теперь их знаменитая система защиты SegFault™ работает безотказно. Или нет.
nc ugractf.ru 5003
Подсказка: источники, близкие к ООО, утверждают, что новый компонент технологии SegFault™ называется «ASLR».
`ucucu.ga/19f/oooverflow2/public/service`

Решение
Атакущий может контролировать первый аргумент функции printf и получить содержимое стека, в том числе адреса возврата.
`ucucu.ga/19f/oooverflow2/WRITEUP.md`

Ответ
`ugra_45lr_is_not_a_pr0bl3m`

Print the input

Программирование, 200 баллов

Авторы задач по программированию думают, что тесты — это абсолютно секретная информация. Поэтому ваши программы они тестируют на разных странных строках: паролях, кодовых словах от своих банковских счетов, и даже на флагах!
Флаг от этого задания расположен в одном из тестов к задаче «Print the input».
Напоминаем, что систему Яндекс.Контест взламывать не надо.
`contest.yandex.ru/contest/12894/problems/2`

Решение
Можно было извлекать полезную информацию из тестирующей системы с помощью стороннего канала — вердикта проверяющей системы.
`ucucu.ga/19f/printinput/WRITEUP.md`

Ответ
`ugra_heck`

Публичные секреты

Криптография, 400 баллов

Пётр снова решил насмешить публику и решил раздавать свои секреты абсолютно бесплатно. Он думает, что никто их не узнает, потому что перед выдачей Пётр шифрует секреты с помощью надежного (судя по одной статье из интернетов) алгоритма RSA. Однако, пытаясь ускорить шифрование, он кое-что упустил... Достаньте его тайное послание:
`nc ugractf.ru 5001`

Решение
Флаг шифровался разными ключами RSA с e = 17. Можно применить Китайскую теорему об остатках для расшифровки флага.
`ucucu.ga/19f/secrets/WRITEUP.md`

Ответ
`ugra_in_elliptic_we_trust`

Turing Complete

Программирование, 200 баллов

Как вы думаете, что такое тьюринг-полный язык?
В любом случае, попробуйте запрограммировать самую настоящую машину Тьюринга.Флаг от этого задания будет доступен на странице «отчёт» после решения задачи «Turing Complete».
`contest.yandex.ru/contest/12894/problems/1`

Решение
Необходимо было просто написать то, что описано в условии задачи, на языке машины Тьюринга.
`ucucu.ga/19f/turing/WRITEUP.md`

Ответ
`ugra_turing_code_magic`