UGRACTF

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

Гостевой режим

Форензика, 50 баллов

Босс «Cybersecure Cybertech Inc.» Пётр очень часто бывает в командировках. В целях экономии средств коллеги используют его компьютер в гостевом режиме. Под видом сотрудников компании наши агенты проникли в офис компании и смогли полностью скомпрометировать всё, в том числе и этот компьютер. Вот файл, который мы получили. Архив зашифрован паролем `uuZ87mRE4jRfLbM2`. Нам нужна твоя помощь в анализе собранных данных. Сотрудники очень часто забывают удалить какие-то важные данные компании после работы за компьютером босса. Проверьте, что вы сможете найти в этот раз.
`ucucu.ga/19q-guest`

Решение
Необходимо понять, что перед нами образ виртуальной машины VirtualBox. В ней есть пользователь без пароля, в домашней директории которого лежит архив с флагом.
`ucucu.ga/19q/guest/WRITEUP.md`

Ответ
`ugra_b055box_ready`

Оперативное расследование

Форензика, 250 баллов

Нам стало известно, что в этот раз босс настолько срочно уехал на деловые переговоры с инвесторами, что оставил все свои приложения открытыми. Но вот незадача — пока мы смогли добраться до компьютера, экран заблокировался. Получается, теперь всё потеряно? Наши эксперты сказали, что этот файл может вам помочь.
`ucucu.ga/19q-logoff`

Решение
Поскольку в условии упоминается состояние системы, воспользуемся фреймворком Volatility и исследуем оперативную память. В ней находим процесс `bash`, с помощью плагина находим команду с выводом флага.
`ucucu.ga/19q/logoff/WRITEUP.md`

Ответ
`ugra_b1g_dump_15_g00d`

Пароль

Форензика, 150 баллов

Пётр заботится о безопасности своих данных, поэтому самые секретные материалы он складывает в директорию суперпользователя, чтобы даже в случае взлома аккаунта никто не смог ничего найти. Но мы уверены, что для тебя это не помеха.

Решение
Мы можем сбросить пароль пользователя root через режим восстановления и получить флаг.
`ucucu.ga/19q/reset/WRITEUP.md`

Ответ
`ugra_r00t_r00t_r00t`

Бэкдор

Форензика, 300 баллов

Антивирусные аналитики ООО «Ты Пывнер» сообщают, что неизвестная хакерская группировка уже давно озаботилась компанией «Cybersecure Cybertech Inc.», и, в частности, заразила файл Петра вредоносной программой для слежения. Конечно же, её нужно обнаружить, потому что её авторы могут обладать важной для нас информацией.

Решение
В файле `~/.xprofile` видим запуск некого JAR-файла. Декомпилируем и находим условие показа флага — секретную переменную окружения.
`ucucu.ga/19q/backdoor/WRITEUP.md`

Ответ
`ugra_linux_java_backdoor`

Try again

Форензика, 300 баллов

Пётр недавно выиграл тендер на обработку конфиденциальной информации. Однако, со слов анонимного источника в компании, на совещании говорили, что партнеры ещё не передали информацию Петру. Возможно, информация появилась после совещания?

Решение
Браузеры сохраняют ссылку, по которой был скачан файл, в расширенных атрибутах, которые читаются утилитой `getfattr`.
`ucucu.ga/19q/tryagain/WRITEUP.md`

Ответ
`ugra_h1dden_a77tribu7es`

Странный вирус

Форензика, 500 баллов

Вирус на компьютере Петра успешно работал лишь короткий интервал времени, однако хакеры успели получить достаточно тайных киберсекретов компании. Однако, они сами совершенно не позаботились о безопасности своих серверов. Поэтому скоро эти секреты получим и мы. Правда же?

Решение
Исследуем уже известный JAR. Он также отправляет нажатия клавиш на сервер. На этом сервере находим открытый порт MySQL. Заходим под анонимным пользователем и получаем флаг.
`ucucu.ga/19q/badvirus/WRITEUP.md`

Ответ
`ugra_mysq1_1n53cur17y`

Елеграм

Форензика, 150 баллов

Для вашего удобства веселья мы подняли воскресили из мёртвых официальный чат. `irc.ugractf.ru`

Решение
Бот отправляет флаг некорректным сервисным сообщением, из-за чего оно не отображается клиентами. Можно снять снимок трафика или пообщаться с сервером через `telnet`.
`ucucu.ga/19q/chat/WRITEUP.md`

Ответ
`ugra_we_are_tired_of_telegram_tasks`

Mystery Book

Программирование, 150 баллов

Есть люди, которые хранят что-то ценное в книгах: деньги, драгоценности, заметки. Однако встречались ли вам те, кто хранит секреты в электронных книгах? Наш клиент именно такой. Стоит убедить его, что киберкниги ничем не лучше обычных.
`thebook.ugractf.ru`

Решение
Каждая буква книги — ссылка. Нужно написать скрипт, который проверит все эти ссылки.
`ucucu.ga/19q/thebook/WRITEUP.md`

Ответ
`ugra_ea5y_f4st_brutef0rce`

CloudFleet

Программирование, 300 баллов

Похоже, нам не удалось убедить нашего клиента в неправоте, и он решил просто защитить свои электронные книги от кибератак. Для защиты он приобрел самую современную систему киберзащиты от сложнейших DDoS-атак от самых продвинутых школьников — CloudFleet®! Покажите, что это абсолютно бесполезно...
`cloudfleet.ugractf.ru`

Решение
Таск похож на Mystery Book, однако после каждого третьего запроса нас блокируют. Необходимо дополнить скрипт использованием публичных прокси-серверов.
`ucucu.ga/19q/cloudfleet/WRITEUP.md`

Ответ
`ugra_unb4n_my_1p_p13453`

Киберсекур

Криптография, 100 баллов

Стартап «Cybersecure Cybertech Inc.» — несомненно, лидирующая киберкомпания по кибершифрованию. Их кибертехнологии опережают время. Подробнее о данной компании можно узнать на официальном представительстве компании в киберпространстве.
`cybersecure.ugractf.ru`

Решение
Сервис шифрует эти строки ключом, участникам требовалось выяснить ключ шифрования.
`ucucu.ga/19q/cybersecure/WRITEUP.md`

Ответ
`ugra_it_was_very_easyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy_task`

Not easy

Криптография, 50 баллов

произошла криптография
`ucucu.ga/19q-noteasy`

Решение
Необходимо было взломать аффинный шифр.
`ucucu.ga/19q/noteasy/WRITEUP.md`

Ответ
`ugra_plez_deccrypt_me_more_more`

Кумир

Реверс-инжиниринг, 150 баллов

Недавно мы нашли необычный файл, похожий на программу на каком-то явно продвинутом и мощном языке программирования.
`ucucu.ga/19q-kumir`

Решение
Нам дан скрипт для исполнителя Черепашка, в котором команды поднятия и опускания пера перепутаны.
`ucucu.ga/19q/kumir/WRITEUP.md`

Ответ
`ugra_turtle_rev3rse`

#лидируйвалидируй

Веб-технологии, 150 баллов

Предлагаем вам лидирующий сервис по валидированию докерфайлов. Пожалуйста, приложите ваш докерфайл к валидатору. Ваш докерфайл — это подтверждение, что ваш контейнер застрахован.
`leadvalid.ugractf.ru`

Решение
В данном таске следовало заметить, что спецификация YAML позволяет исполнять код при небезопасной загрузке.
`ucucu.ga/19q/leadvalid/WRITEUP.md`

Ответ
`ugra_ule_ele_valilele_trali_vali_validate`

Игроман

Сетевая разведка, 100 баллов

Антон очень любит старые игры. Мы сделали фото у него дома.
Всем известно, что Антон шифрует все свои заметки на этом сайте.
Но где же взять пароль?
`ucucu.ga/19q-nes`
`encipher.it?EKYA`

Решение
Необходимо было найти игру с монитора и пройти её, используя код со стикера. После прохождения мы получали пароль от заметки.
`ucucu.ga/19q/nes/WRITEUP.md`

Ответ
`ugra_r37r0g4m1ng_f4n_31337`

Ученый

Стеганография, 75 баллов

Учёный Иннокентий решил отправить свою первую статью в известный научный журнал.
Нам эта статья кажется немного странной.
`ucucu.ga/19q-scientist`

Решение
В данном задании был дан PDF-файл со скрытой картинкой-вложением.
`ucucu.ga/19q/scientist/WRITEUP.md`

Ответ
`ugra_its_not_an_embedded_file`

Странная страница

Веб-технологии, 150 баллов

Недавно на просторах интернета мы нашли странную страницу, которая, кажется, выглядит по-разному на разных мониторах.
`strange.ugractf.ru`

Решение
При разной ширине экрана те или иные элементы флага скрываются. Необходимо изменить @media-правила так, чтобы все элементы были показаны.
`ucucu.ga/19q/strange/WRITEUP.md`

Ответ
`ugra_rugau_ucucugu_a_ragu_ug`

Trash can

Сетевая разведка, 150 баллов

В свободное время Пётр смотрит видео на популярном видеохостинге YouTube.
Ещё больше, чем смотреть, Петру нравится комментировать. Однако, чтобы не портить престиж компании, он это делает с фейкового аккаунта.
Нам сообщили, что недавно видели его комментарий под этим видео, но мы не смогли его обнаружить.
Может быть тебе это удастся?
`youtu.be/vtqtyyGZvXM`

Решение
Необходимо воспользоваться API YouTube и извлечь все комментарии к видеоролику, после чего найти среди них нужный.
`ucucu.ga/19q/trash/WRITEUP.md`

Ответ
`ugra_l33ty_flooder`