NSK School CTF 2017 - 25 марта 2017

Разбор заданий

Категория ADMIN

100

- **Задание**: Как называется символ(группа символов) в начале скрипта на bash? Flag: CTF{answer}
- **Ответ**: CTF{shebang}
- **Решение**: гуглим вопрос

200

- **Задание**: В Global ind. данный тест проходят на собеседовании на должность помощника сис.администратора,попробуйте пройти и вы,это может помочь узнать больше о данной компании https://yadi.sk/d/CW7c9Cbl3F4ebx
- **Ответ**: CTF{Tux_1s_f4m0u5_b1rd}
- **Решение**: В тесте предлагалось 5 вопросов. Трудности возникли с последним - отцом Linux'a. Им был Linus Torvalds, необходимо было написать ответ слитно

300

- **Задание**: Вы в офисе компании Global ind.,заигрываете с секретаршей Кейт,что бы получить нужую вам информацию и вдруг у нее внезапно перестает открываться ее любимый сайт с котятками.Верните ей доступ в интернет,чтобы произвести на нее впечатление (Внимание!!! для данного задания используется образ диска от предыдущего задания)
- **Ответ**: CTF{c0nn3ct10n_i5_p0w3r}
- **Решение**: После загрузки в систему видим, что Интернет на машине отсутствует. Пытаемя его включить командой `ifup eth0` (или eth1). Не выходит. Смотрим настройки сети в /etc/network/interfaces - файла нет. Придётся нам его восстанавливать. Прописать настройки необходимо было такие: `auto eth0 \n iface eth0 inet dhcp`. После этого необходимо было сохранить данный файл, перезагрузить менеджер сети `sudo service networking restart && sudo service network-manager restart`, поднять интерфейс eth0 командой `ifup eth0`, после чего сервер успешно получал интернет, подключался к удалённому серверу и скачивал файл с флагом

400

- **Задание**: Я потерял свой докерфайл. Помогите его восставновить. Я помню только примерную структуру.Структура описана в файле description.txt https://school.nskctf.ru/files/admin/admin400.zip
- **Ответ**: CTF{05D867F0AE202D1FC48672EB58FBD878}
- **Решение**: Необходимо было настроить Dockerfile верным путём. Правильно собранный файл находится в папке /admin/admin400.zip

Категория CRYPTO

100

- **Задание**: И это вы называете крутым паролем? - после этой фразы наш человек взломал сервер банка. Попробуйте и вы.
  `Q1RGe2RvX3lvdV9zZWVfYmFzZTY0X2Zvcl90aGVfZmlyc3RfdGltZX0=`
- **Ответ**: CTF{do_you_see_base64_for_the_first_time}
- **Решение**: decrypt base64

200

- **Задание**: Система шифрования данных у них - просто блеск! - После этой фразы были дешифрованы секретные документы. https://school.nskctf.ru/files/crypto/Crypto200.docx
- **Ответ**: CTF{Thls_ls_CeZaR}
- **Решение**: Перед участниками 2 картинки и зашифрованный текст. На первом изображении салат Цезарь, значит будет шифр Цезаря. На второй арифметическия задачка с фруктами. Решив ее, мы получим число 16. Это шаг, который использовался при шифровании. Остается расшифровать текст и выписать флаг.

300

- **Задание**: Возможно, вам что-то хотят сказать https://school.nskctf.ru/files/crypto/crypto300.zip
- **Ответ**: CTF{simple}
- **Решение**: Обычный Морзе, долгое свечение - тире, короткое - точка. Закидываем декодер Морзе - получаем ответ

400

- **Задание**: https://school.nskctf.ru/files/crypto/crypto400.cpp У вас есть все, чтобы найти ключ: алгоритм, исходное(hellomyfriend) и зашифрованное(KxhrwFrAAnrnA)
- **Ответ**: CTF{szomurzjvsfxh}
- **Решение**: Необходимо проверить синус разницы букв ASCII(исходного и ключа при том, что буква ключа больше, чем исходного сообщения. Из полученного цикла необходимо сложить 5 цифр после запятой. Это число+97, и если получается ASCII зашифрованного сообщения,

то буква найдена. Подробное решение от автора лежит в файле `crypto/crypto400 Решение.doc`

500

- **Задание**: https://school.nskctf.ru/files/crypto/crypto500.zip У нас есть важные данные, и естественно они зашифрованы (файл 0-без формата). Помогите нам это исправить
- **Ответ**: CTF{CrYPT0_Zl0_For_CtF!}
- **Решение**: Здесь был представлен специфический криптографический алгоритм, написанный на PHP. Файл 0 - ключ. Решение алгоритма представлено в архиве crypto/500.zip

Категория FORENSIC

100

- **Задание**: Нам пришло странное письмо, с одной единственной ссылкой... http://nsks.torpress2sarn7xw.onion/
- **Ответ**: CTF{It_is_darknet!}
- **Решение**: http://nsks.torpress2sarn7xw.onion/ Участнмикам дана ссылка выше. Нужно перейти по это ссылке, используя браузер Tor. На этом сайте лежит флаг.

200

- **Задание**: У одного из наших боссов украли телефон с важной информацией. К счастью, наши спецы быстро вернули его обратно. А вы сможете? Flag:CTF{name_of_city} https://yadi.sk/i/pRd4tqqg3G9yCj
- **Ответ**: CTF{Glendale}
- **Решение**: Картинка в jpeg. Открываем метаданные о ней. Exif -> geo

300

- **Задание**: Кажется, это голосовой слепок от замка. Нужно понять, кто автор этого "произведения"... Flag: CTF{} https://yadi.sk/d/Qp__5Wyv3G9yDY
- **Ответ**: CTF{Rick_Astley}
- **Решение**: Audacity-reverse. Необходимо замедлить песню и развернуть её. Тогда вы услышите знаменитую песню Never gonna give you up от Rick Astley

Категория PPC

100

- **Задание**: https://school.nskctf.ru/files/ppc/ppc100.zip
- **Ответ**: CTF{flag112galf}
- **Решение**: Авторское решение довольно объёмное, сюда не влезло. Вы можете посмотреть его в файле ppc/ppc100.zip

200

- **Задание**: Мистер Персонаж - очень азартный человек, он любит покер, играть на ставках и просто обожает заключать пари по любому поводу. На этот раз, желание поспорить настигло его на встрече с давним хорошим другом, работающим программистом в компании Giigli. В течение всей беседы, Мистер программист воодушевленно и с жаром рассказывал ему о прорывах современных технологий, о невероятных достижениях искусственного интеллекта, о создании новейшего позитронного мозга и вместе с тем о большом скачке в развитии робототехники. В пылу обсуждений, программист обмолвился об инновационной разработке сверх-мощного и непобедимого игрока в камень/ножницы/бумага - Fobos-0189, заявив, что его никто и никогда не сможет обыграть. Мистер персонаж, не долго думая, решил бросить вызов роботу. Обдумав, он понял, что для победы честным способом ему потребуется слишком много времени... Внезапно, он вспомнил, что не так давно все спецслужбы были подняты на ноги из-за многочисленных кибер-атак группы хакеров, именующей себя L1f3. Путем сложных умозаключений и напряженной мыслительной деятельности, мистер Персонаж догадался, как можно выйти на связь с этой группой. Оказалось, что хакеры тоже весьма азартны, поэтому они с удовольствием согласились помочь ему. Насколько мы слышали, ты тоже один из них поэтому даем тебе данные для доступа nc 5.8.180.250 80
- **Ответ**: CTF{W0O0W_Y0uu_w1n_nn3}
- **Решение**: Решение данного задания, а также сам сервис для игр доступен в файле ppc/ppc200.rar

300

- **Задание**: Накануне Нового Года и праздничных каникул людям не терпится улететь из холодной страны, и семья Мистера Персонажа не оказалась исключением. Его горячо любимая сестра Миссис Рест, бросив в чемодан купальник и поцеловав на прощание в щеку мистера Персонажа, улетела навстречу пальмам и теплому морю, оставив ему под присмотром квартиру, двух котов и еще не закончившего учебу сына. Как выяснилось, племянник Мистера персонажа не особо проявляет рвение к учебе, но зато просто обожает свою приставку вместе с новенькой GuitarHero и может играть в нее часами напролет. Тогда в мозгу мистера Персонажа возникла изящнейшая комбинация. В ближайший же вечер за ужином он сказал - \"Слушай, маленький оболтус, у меня есть к тебе отличное предложение! За эту неделю я с нуля обучусь твоей игре и мы устроим соревнования в ближайший уикенд. Победишь ты - я весь год буду решать твои домашние задания, ну а если

выиграю я - у меня на территории есть прекрасный газон, который тебе придется стричь.\"Целый год свободы от учебы... Да и к тому же я лучший игрок в своем дворе!\" - подумал малолетний и искушенный племянник и, не почуяв подвоха, сразу же согласился. У Мистера Персонажа никогда не было ни приставки, ни ловкости рук, но зато была смекалка и старый добрый друг мистер Программист, под контролем которого создавались новейшие изобретения кибер техники.

- **Ответ**: CTF{Rick_Astley}
- **Решение**: Реализуем обработку последней строки и отправляем на сервер необходимые символы. Решение данного задания, а также сам сервис для игр доступен в файле ppc/ppc300.rar

400

- **Задание**: Мистер Персонаж, после длинной череды побед в своих пари, на которых смог заработать целое состояние, наконец то исполнил свою заветную мечту - переехал в новый прекрасный район, с множеством скверов, фонтанов и спортивных площадок. Среди всего этого великолепия размещаются 255 домов, которые соединены между собой живописными пешеходными дорожками. Причем, каждая из них имеет свою длину. Счастливый Мистер обживает свою новую уютную квартиру в доме под номером 67, а его друг детства купил себе квартиру неподалеку, на тенистой аллее - в доме 82. Так как оба они люди веселые и жизнерадостные, то часто устраивают совместные вечеринки. Как человек творческий, Мистер каждый раз добирается до своего друга разными путями. Из-за этого своего свойства, он часто опаздывает к началу празднования. Чтобы в дальнейшем избежать таких досадных инцедентов, Мистер хочет нарисовать подробную карту, на которой сможет найти короткий путь до жилища друга. Но при этом он не хочет, чтобы кто-то еще смог прочитать эту карту и прийти раньше него. Поэтому, в целях конспирации, он решил вместо цифр обозначать путь символами индейцев Майя. Мистер знает все пути, но, как гуманитарий, не понимает, как из всего этого выбрать кратчайший путь!
- **Ответ**: CTF{CtF_iT[lz^eaSy~VErY:n1c3\ANsv9R}
- **Решение**: Реализуем обход в ширину по графу и получаем кратчайший путь, затем переводим в ascii символы и получаем флаг

Категория STEGO

100

- **Задание**: Мы перехватили сообщение от соседней группировки, подозрительно что они вдруг стали общаться картинками. https://school.nskctf.ru/files/stego/stego100.jpg
- **Ответ**: CTF{l6_wanT_To_plAY}
- **Решение**: Флаг уже немного видно при открытии картинки. Но её можно прогнать через StegSolve или открыть в Photoshop и поиграться яркостью/контрастностью

200

- **Задание**: Иногда, файлы нужно прятать. https://school.nskctf.ru/files/stego/stego200.zip
- **Ответ**: CTF{StEg0_1$_C0minG}
- **Решение**: Открываем картинку. На ней видим значения хекса - это отсылка к тому, что надо смотреть файл в хексе. В хексе находим, что под картинкой лежит архив 7z с 3 файлами. Вырезаем из под картинки архив или открываем ее архиватором. В архиве лежит 3 файла, GIF, JPG, PNG. Картинки подобраны по критерию "Рекурсия" - отсылка, что принцип решения тот же. Gif лежит для массовки. Под Jpg и Png лежат архивы. Под Jpg лежит архив с паролем, от архива под Png, в виде простого математического уровнения. В запороленном архиве лежит флаг.

300

- **Задание**: Кажется, от нас опять пытаются что то скрыть... https://school.nskctf.ru/files/stego/stego300.mp3
- **Ответ**: CTF{SEcreT_FlaG}
- **Решение**: Видим обложку аудиофайла, извлекаем картинку. В картинке находится архив с флагом

400

- **Задание**: О, щас будет дискотека! Хотя, стоп... https://yadi.sk/d/ffiuJbmU3G7X8i
- **Ответ**: CTF{HALF_the_ANSWER}
- **Решение**: Имеется 2 файла формата .wav. Открываем аудиофайлы с помощью virtual ans. Видим что написанны непонятные символы: в 1.wav верхняя половина букв, в 2.wav нижняя половина букв. Соединяем и получаем флаг

Категория WEB

100

- **Задание**: Похоже, защита у этого банка, мягко говоря, хромает... http://web100.school.nskctf.ru/
- **Ответ**: CTF{S0_e@$y_W3b}
- **Решение**: Source code -> password

200

- **Задание**: Хм, похоже они пофиксили что то. Или нет... http://web200.school.nskctf.ru/
- **Ответ**: CTF{|0v3J@v@$cr!p[_s0_m@c][}
- **Решение**: JS -> Массив -> Пароль

300

- **Задание**: Возможно, вам что-то хотят сказать https://school.nskctf.ru/files/crypto/crypto300.zip
- **Ответ**: CTF{kP94QcYA73ncS}
- **Решение**: гуглим PHP Magic Hashes. https://www.whitehatsec.com/blog/magic-hashes/. подходит: 240610708

400

- **Задание**: Большой брат следит за тобой. Узнай, как он это делает, и дай отпор! http://web400.school.nskctf.ru/
- **Ответ**: CTF{MhLTxMS3KuhJS}
- **Решение**: Данные о просмотрах записываются в MySQL-базу из cookies. Нужно было произвести обычную MYSQL-инъекцию в User-Agent (данные вашего браузера) и заменить весь текст User-agent на `'+OR+1=1--`. Тогда выводится ваш флаг

500

- **Задание**: Один из главарей преступной группировки DedSec создал страничку, где хранит крайне важную информацию. Но мы не знаем его ник! Найди его, и мы попытаемся деанонимизировать этого негодяя

http://web500.school.nskctf.ru/

- **Ответ**: CTF{NoSQLInjectionExample}
- **Решение**: Nosql-injection. Отправляем POST-запрос с параметрами user[$gt] и pass[$gt] вместо user и pass на наш сервер - пароль получен! Пример взят отсюда http://blog.websecurify.com/2014/08/hacking-nodejs-and-mongodb.html