УДК 004.056.4

ОБЗОР СОРЕВНОВАНИЙ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ CTF

Д.О. Жукова
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В статье представлены и рассмотрены примеры заданий из различных областей информационной безопасности, затрагиваемые при проведении соревнований по компьютерной безопасности CTF. Рассмотрена роль подобных соревнований в обучении специалистов информационной безопасности.
Ключевые слова: соревнования, безопасность, информационная, роль, специалисты

Введение

В условиях быстрого роста информатизации общества возникает проблема безопасности компьютерных систем. В связи с этим очень важна подготовка квалифицированных специалистов по защите информации. Одной из возможностей получения навыков в данной области является участие в соревнованиях по компьютерной безопасности. Capture The Flag дословно переводится как «захват флага». В компьютерной безопасности под «захватом флага» подразумевают командные соревнования, целью которых является оценка умения участников атаковать и защищать компьютерные системы. Каждая команда получает выделенный сервер или небольшую сеть для поддержания её функционирования и защиты. Во время игры команды получают очки за корректную работу сервисов своего сервера и за информацию (флаги), полученную в результате использования уязвимостей сервисов других участников. Подобные соревнования позволяют участникам закрепить практические навыки, обменяться опытом в области компьютерной безопасности и дают существенный импульс для профессионального роста их участников. Первые удалённые международные межвузовские соревнования iCTF UCSB были проведены университетом Калифорнии, город Санта-Барбара в 2004 году. Участникам необходимо было проявить знания в таких областях, как анализ машинного кода программы (reverse engineering), анализ входящего и исходящего трафика (network sniffing), анализ протоколов (protocol analysis), системное администрирование, программирование, криптоанализ, стеганоанализ. Подобные соревнования проводятся и в России и проходят в два этапа.

Отборочные соревнования

В настоящее время значение стеганографии в компьютерном мире в полной мере не оценено, в связи, с чем этот метод защиты информации является недостаточно развитым. В отличие от криптографии, стеганография не просто засекречивает передаваемое сообщение, а скрывает сам факт его передачи. Организаторы конкурса CTF, используя метод стеганографии зашифровали некоторую фразу в изображении (рис. 1).

Рис. 1. Изображение с засекреченным сообщением

Для успешного решения данного задания следовало подобрать необходимую яркость изображения (рис. 2), затем обратить цвета, применить некоторые специализированные фильтры для работы с изображениями и получить так называемый бар-код – штрих-код в двухмерном формате (рис. 3).

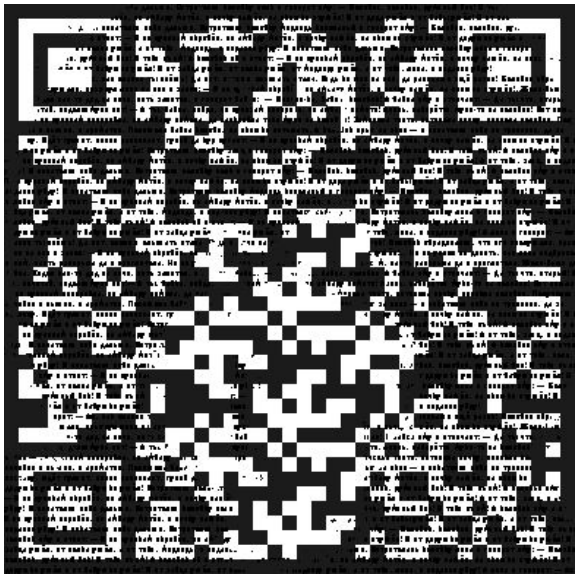

Рис. 2. Изображение после изменения яркости

Рис. 3. Полученный бар-код

После использования программы для расшифровки бар-кодов ZXing Decoder был получен результат – сообщение «JURY LIKES VERY LITTLE PENGUINE DISTROS».

В данном задании стеганография используется совместно с криптографией, что является очень мощным методом передачи секретной информации.

Из рамок цифровой стеганографии вышло наиболее востребованное легальное направление – встраивание цифровых водяных знаков (ЦВЗ), являющееся основой для систем защиты авторских прав и DRM (Digital rigts management) систем. Методы этого направления настроены на встраивание скрытых маркеров, устойчивых к различным

преобразованиям контейнера (атакам).

На RuCTF2009 участникам было необходимо найти ЦВЗ в следующем изображении:

Рис. 4. Изображение со встроенным ЦВЗ

Ни одна из существующих программ распознавания не могла помочь в нахождении ЦВЗ в этом изображении. В качестве подсказки к данному заданию была дана программа, с помощью которой этот ЦВЗ был вставлен в картинку. Следовало дизассемблировать данную программу, после чего можно было увидеть алгоритм встраивания ЦВЗ, и соответственно, следуя алгоритму, обнаружить сам цифровой водяной знак. Сложность удаления подобного рода защиты изображений от копирования говорит о надежности данного метода защиты авторских прав.

Финальный этап

Во время финала каждая команда получает от жюри сервер с предустановленным набором уязвимых сервисов. На момент начала игры сервера команд идентичны. Задачи участников: поддерживать свои сервисы в рабочем состоянии, предотвращать попытки вторжения и проводить аудит серверов других команд. Командам необходимо обнаружить уязвимости на своем сервере и попытаться закрыть их, не нарушив работоспособности сервисов. В то же время, используя знания о найденных уязвимостях, становится возможным провести аудит состояния уязвимостей у других команд. На финальном этапе можно выделить два основных направления, на которые участникам следует обратить особое внимание.

1. Поиск уязвимостей. Поиск уязвимостей необходимо проводить как с использованием инструментальных средств (сканеров безопасности), так и вручную (reverse engineering).

2. Закрытие найденных уязвимостей, которое заключается в исправлении ошибок, найденных в исходном коде сервиса, либо путем написания эксплоита для закрытия существующих уязвимостей в нужном сервисе.

Заключение

Участие в соревнованиях подобного рода имеет огромное значение для изучения методов защиты информации на практике. Следует учитывать важность проведения таких соревнований среди студентов, так как они дают возможность применить полученные в процессе обучения навыки на практике, опробовать существующие методы обеспечения информационной безопасности в условиях, приближенных к реальным, а также в полной мере оценить всю сложность и важность защиты информации, компьютерных и телекоммуникационных систем в современном мире.