**Задания I внутривузовского соревнования МГТУ по task-based CTF**

1. **Admin.**
   1. Unlabel

**Необходимые знания и навыки:**

-Умение работать по SSH;

или

-Умение работать с bash;

**Реализация:** создается виртуальная машина с измененной раскладкой клавиатуры. Флаг находится у пользователя прямо под носом, но вот скопировать или заглянуть в него – задача не из легких. Изначально ssh не установлен, но его при желании можно установить. Как команда на установку ssh так и команда на изменения раскладки оставлены в истории bash.

**Условия задания:** дан путь к файлу. Получить флаг.

* 1. Unable

**Необходимые знания и навыки:**

-Умение работать по SSH

-Умение работать с bash

-Знание скриптового языка программирования

**Реализация:** создается виртуальная машина. Пользователю доступна только одна команда в режиме sudo, а именно, команда, возвращающая случайный байт из указанного файла. У пользователя есть доступ к директории, но не к файлам. В директории много файлов, но в них всего по два байта. Имена файлов – позиции байтов в тексте.

**Условия задания:** дан путь к директории с файлами. Получить флаг.

* 1. Unstable

**Необходимые знания и навыки:**

-Умение работать по SSH

-Умение работать с bash

-Знание MySQL

**Реализация:** создается виртуальная машина. В системе запущен nginx от ctfuser, конфиг к которому слит пользователю. У nginx’а есть доступ и к папке, и к файлу. Файл размером ~1Gb – содержит данные в формате CSV, а именно, какие-то строки и хеши к ним и несколько колонок с ненужной информацией. Необходимо найти ту строку, в которой хеш окажется неверен. Скорость сетевого интерфейса виртуальной машины ограничена, более того она перезагружается через заданные промежутки времени.

**Условия задания:** дан путь к директории. Получить флаг.

1. **Crypto.**
   1. Keys under the floorboards.

**Необходимые знания и навыки:**

-Умение работать с SSL.

**Реализация:** необходимархив с набором открытых ключей формата pem. Консольная программа, получающая закрытый ключ по payload’у открытого ключа.

**Условия задания:** дан архив с открытыми ключами. Найдите backdoor и используйте его.

* 1. Fermat is displeased with your cryptosystem.

**Необходимые знания и навыки:**

-Знание алгоритма RSA, его сильных и слабых сторон.

-Знание алгоритма факторизации Ферма.

-Навыки анализа входящего трафика (сниффинг).

**Реализация:** необходим веб-сервис отправляющий открытый ключ RSA с определенной периодичностью.

**Условие задания:** нужно перехватить открытый ключ и при помощи него получить закрытый.

* 1. Et tu, Brute?

**Необходимые знания и навыки:**

-Навыки Hash crack’инга.

-Знание шифра Бэкона.

-Знание алгоритма шифрования Base64.

-Умелое использование Bruteforce.

**Реализация:** необходим лист с зашифрованными сообщениями.

**Условие задания:** требуется расшифровать сообщения, которые в итоге составят ключ.

1. **Exploit.**
   1. Oh, God, I’m bleeding!  
        
      **Необходимые знания и навыки:**

- Умение работать с UNIX;

- Понимание основ работы OpenSSL и протокола TLS.

**Реализация:** установка на сервере ПО OpenSSL версии 1.0.1, создание пользовательской учетной записи и смена у него пароля каждые 15 минут. В домашней директории лежит файл с ключом.

**Условие задания:** требуется провести атаку на сервер, заполучить данные пользователя и получить ключ.

* 1. Shell compromised.  
       
     **Необходимые знания и навыки:**

- Знание CGI на базовом уровне;

- Начальные знания HTTP и JSON;

- Средний уровень знаний python.

**Реализация:** настройка веб-сервера с сервисом, предоставляющим доступ с программной оболочке python. Ответом на запросы будет JSON строка. Создание модуля python, имеющему уязвимость, позволяющую пользователю подгрузить на сервер собственный скрипт. Флаг хранится в $HOME, в зашифрованном виде. Расшифровать можно, используя подгруженные по умолчанию модули.

**Условие задания:** провести атаку на сервер, используя CGI интерфейс. Ответом будет флаг из файла.

1. **Joy.**

4.1. Где же ключ?

**Необходимые навыки**:

- Находчивость;

- Смекалка;

- Нестандартное мышление.

**Реализация:** в правилах конкурса, в месте, где приводится пример с ключом, указать в качестве примера определенный «ключ». Он и будет ответом к самому заданию.

**Условие задания:** Прочтите правила и приступайте к заданиям. Первый флаг у Вас перед носом.

4.2. Москва в Париже.

**Необходимые навыки:**

- Находчивость;

- Умения работать с гео-тегами в файлах.

**Реализация**: проверка правильности выполнения задания заключается в оценке результирующего файла, который представляет собой фотографию, на которой запечатлена какая-либо достопримечательность Москвы, а в геотегах (которые можно будет проверить, например, при помощи программы ACDsee) будут стоять координаты любого места в Париже.

**Условие задания**: Сфотографируйте Москву в Париже.

1. **Reverse.**
   1. Simple auth.  
        
      **Необходимые навыки и знания**:  
      - Начальные знания asm;  
      - Начальные знания симметричного кодирования;  
      - Понимание основ программирования на Си/Си++;  
      - Опыт работы с программами-дизассемблерами, например, IDA.  
        
      **Реализация:** разработать консольную программу на Си++, которая последовательно принимает на вход два пароля: первый проверяется с использованием функции *strcmp*, ко второму предварительно применяется симметричное шифрование по магическому квадрату Дюрера. После успешной проверки паролей требуемую информацию *data* вывести в модальном окне, предварительно расшифровав простым xor’ом с конкатенацией двух паролей.  
        
      **Условие задания:** Дан исполняемый файл с расширением exe, который является программой и представляет из себя простую систему аутентификации. Требуется подобрать 2 пароля (*pass1*, *pass2*) для доступа к информации (*data*). Ответом на задание является строка *pass1\_pass2\_data*.
   2. It’s l33t time.  
        
      **Необходимые навыки и знания:**  
      - Знание «кодировки» Leet (1337, L33T, L337);  
      - Базовые знания о форматах исполнимых файлов (в частности, формат Mach-O);  
      - Базовые знания о стеке протоколов, структуре пакетов, raw-пакетах;  
      - Опыт работы с программой Wireshark;  
      - Уверенное пользование дизассемблером.  
        
      **Реализация:** разработать программу на Си++, которая открывает socket, связывает ip и port, и слушает входящие пакеты. При установлении tcp-соединения программа получает данные для шифрования/дешифрования, затем вызывается функция XOR, которая производит in-place побайтовый XOR с ключом, который является записью текущего времени в формате hhmm. В ответ на запрос клиента, программа отправляет tcp-пакет с расшифрованными данными. Программа вернет флаг в случае, если текущее время – 13:37.  
        
      **Условия задания:** Даны два файла: файл без расширения и дамп пакетов c расширением pcap. Требуется отыскать флаг.
   3. Hello, Server, it’s me.  
        
      **Необходимые навыки и знания:**- Базовые знания о стеке протоколов, структуре пакетов, raw-пакетах;  
      - Знание какого-либо скриптового языка;  
      - Уверенное пользование дизассемблером;  
      - Опыт использование отладчика gdb.  
        
      **Реализация:** разработать консольную программу на Си++, которая принимает на вход 2 аргумента (key/value) и возвращает True в случае соответствия пары и False – в противном случае. Проверку аргументов максимально усложнить, используя сложные математические функции. Программу скомпилировать под Unix-подобные системы. Кроме того, разработать программу для сервера, которая будет работать в следующем режиме: при подключении клиента отправляет ключ (key) и ждет значение (value) от клиента, который должен соответствовать ключу (если подать данные отправленные сервером и клиентом на вход консольной программы, она должна выдать True). В случае успеха сервер генерирует случайным образом новый ключ, иначе – ответ сервера повторяется. После 100 успешно подобранных пар, сервер отправляет только флаг.  
        
      **Условие задания:** дан файл check.elf, ip и port сервера. Подберите значения для всех ключей, чтобы получить флаг.
2. **Steganography.**

6.1. Pay attention.

**Необходимые знания и навыки:**

- Знание стеганографии;

- Умение работать с компьютерной графикой;

- Умение работать в Adobe Photoshop на базовом уровне.

**Реализация:** создать два одинаковых растровых изображения с глубиной цвета 12 bpp или 32 bpp, в одном из изображений отредактировать некоторые элементы так, чтобы 4 отличия были видно налицо, а пятое заключалось в следующем: в битовых представлениях некоторых цветов изменить биты на противоположные так, чтобы оттенок цвета почти не изменился, а при наложении (XOR-е) двух изображений получался необходимый флаг. **Условие задания:** даны два изображения, найти 5 отличий, последним из которых будет являться флаг, зашифрованный в одном из изображений.

6.2. Hear me in the eye.

**Необходимые знания и навыки:**

- Умение работать в звуковых мультиредакторах;

- Знание python.

**Реализация:** создать (взять готовый) аудиофайл, с помощью аудиоредактора открыть его частотный спектр, спрятать флаг в недра спектра.

**Условие задания:** дан аудиофайл, получить из него флаг. Варианты исполнения:   
1) открыть частотный спектр аудиофайла в аудиоредакторе (e.g. Audacity), найти флаг в недрах спектра.

2) найти оригинал аудиофайла, наложить аудиофайлы, написать программу для получения флага.

1. **Web.**

7.1. Inexpert admin.

**Необходимые знания и навыки:**

- Знание стандартных уязвимостей сайтов;

- Знание различных методов кодирования.

**Реализация:** создать сайт с «Predictable Resource Location»-уязвимостью и с возможностью составления логики в обработке пароля через браузерную строку, участник найдя логин администратора, заходит под ним на сайт, среди данных будут храниться все пары логин-пароль, причем пароль будет закодирован в Base64, одна из таких пар будет содержать искомый флаг.

**Условие задания:** предоставлен сайт, получить флаг, хранящийся в данных администратора сайта.

7.2. Divide and rule.

**Необходимые знания и навыки:**

- Знание стеганографии;

- Знание различных методов кодирования;

- Знание методов шифрования с открытым ключом;

- Умение проводить анализ Web-страниц.

**Реализация:** создать текст, содержащий описание задания и части ключа, с использованием стеганографии, зашифровать его методом шифрования с открытым ключом и поместить в текстовый файл; создать архив с хранящейся в нем ссылкой на Web-страницу, поставить на нем защиту в виде пароля, создать сайт с авторизацией, при правильной авторизации сайт переходит на страницу со второй частью ключа(правильной авторизацией считается пара логин-пароль, где логин – название команды, пароль – пароль от защищенного архива), при неправильной авторизации сайт переходит на страницу, в коде которой хранится третья часть ключа, при просмотре на сайте запрещенных для поисках запросов будет наблюдаться четвертая часть, после их объединения и применения декодировки из Base64 участники получают искомый флаг.

**Условие задания:** предоставлены два файла: текстовый и архив с паролем; получить флаг, состоящий из 4 частей.