1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 5**

1. **«Анализ локального DNS-сервера»**
2. по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности»
3. Выполнил
4. студент гр. 5151004/10101 Плохотникова М.С.

<*подпись*>

1. Проверил
2. преподаватель Семенов П.О.

<*подпись*>

1. Санкт-Петербург
2. 2024

# Цель работы

Проанализировать параметры и заголовки запросов и ответов к локальному DNS-серверу. Определить уязвимые места.

# ход решения

## Анализ запросов к удаленному сайту, ранее не открывавшемуся

В качестве существующего сайта был выбран сайт иркутского ледового дворца (https://iceberg38.ru/), к которому ранее не было обращений. Среди DNS пакетов были найдены записи типа A, которые сопоставляют домену связанный с ним IPv4-адрес.

Изображение выглядит как текст, снимок экрана, Шрифт, информация

Автоматически созданное описание

Рисунок 1 – DNS-пакеты для разрешения имени iceberg38.ru

Изображение выглядит как текст, Шрифт, число, линия

Автоматически созданное описание

Рисунок 2 – DNS-запрос на разрешение имени iceberg38.ru

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 3 – DNS-ответ для разрешения имени iceberg38.ru

## Анализ запросов к очень удаленному сайту

В качестве далеко удаленного сайта был выбран сайт правительства Франции (https://www.info.gouv.fr/).

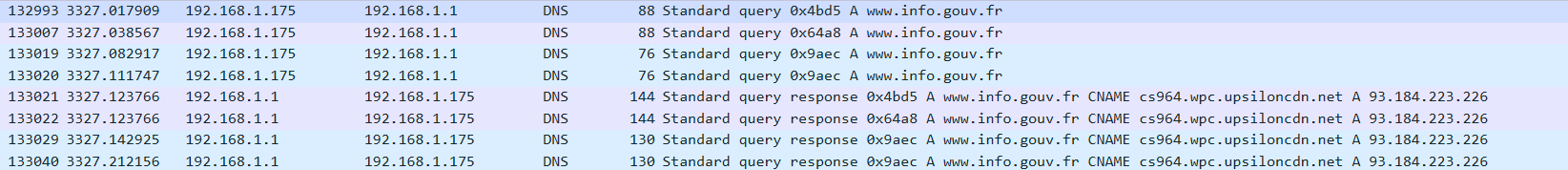


Рисунок 4 – DNS-пакеты для разрешения имени www.info.gouv.fr

Изображение выглядит как текст, снимок экрана, Шрифт, алгебра

Автоматически созданное описание

Рисунок 5 – Цепочка DNS-ответов

## Анализ запросов к несуществующему сайту

В качестве несуществующего сайта было выполнено обращение к домену baddomain.fetch.com. В качестве результата пришел ответ с кодом 3 в Reply code, что говорит о ненайденном имени.

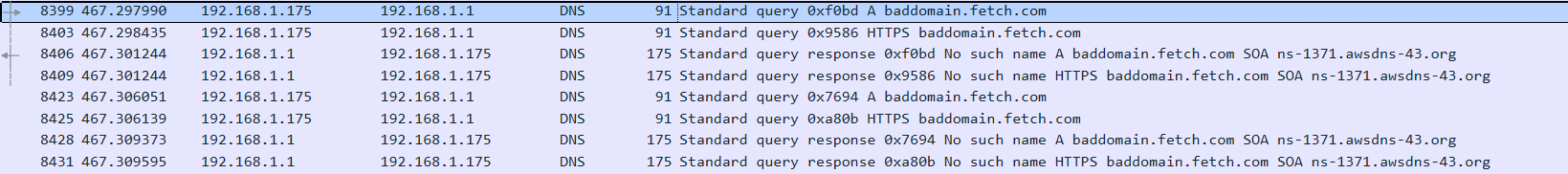


Рисунок 6 – Попытка найти ip адрес несуществующего сайта

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 7 – Ошибка в DNS-ответе о несуществующем домене

## Структура заголовка DNS-пакета

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 8 – Структура заголовка DNS-пакета

* ID (16 бит) — данное поле используется как уникальный идентификатор транзакции. Указывает на то, что пакет принадлежит одной и той же сессии “запросов-ответов” и занимает 16 бит.
* QR (1 бит) — данный бит служит для индентификации того, является ли пакет запросом (QR = 0) или ответом (QR = 1).
* Opcode (4 бита) — с помощью данного кода клиент может указать тип запроса, где обычное значение:

0 — стандартный запрос,

1 — инверсный запрос,

2 — запрос статуса сервера.

3-15 – зарезервированы на будущее.

* AA (1 бит) — данное поле имеет смысл только в DNS-ответах от сервера и сообщает о том, является ли ответ авторитетным либо нет.
* TC (1 бит) — данный флаг устанавливается в пакете ответе в том случае если сервер не смог поместить всю необходимую информацию в пакет из-за существующих ограничений.
* RD (1 бит) — этот однобитовый флаг устанавливается в запросе и копируется в ответ. Если он флаг устанавливается в запросе — это значит, что клиент просит сервер не сообщать ему промежуточных ответов, а вернуть только IP-адрес.
* RA (1 бит) — отправляется только в ответах, и сообщает о том, что сервер поддерживает рекурсию
* Z (3 бита) — являются зарезервированными и всегда равны нулю.
* RCODE (4 бита) — это поле служит для уведомления клиентов о том, успешно ли выполнен запрос или с ошибкой.

0 — значит запрос прошел без ошибок;

1 — ошибка связана с тем, что сервер не смог понять форму запроса;

2 — эта ошибка с некорректной работой сервера имен;

3 — имя, которое разрешает клиент не существует в данном домене;

4 — сервер не может выполнить запрос данного типа;

5 — этот код означает, что сервер не может удовлетворить запроса клиента в силу административных ограничений безопасности.

* QDCOUNT(16 бит) – количество записей в секции запросов
* ANCOUNT(16 бит) – количество записей в секции ответы
* NSCOUNT(16 бит) – количество записей в Authority Section
* ARCOUNT(16 бит) – количество записей в Additional Record Section

## Недостатки с точки зрения возможных атак

1. Флаг авторизации (AA) был проинициализирован нулем, что свидетельствовало о получении неавторизированного ответа. Это может означать, что ответ получен из кэша, который может быть устаревшим или скомпрометированным.
2. Флаг Answer Authenticated опущен, что означает, что сервер не проверял подлинность ответа, полученного от другого сервера. Злоумышленник может использовать DNS-запросы для скрытой передачи данных, так как сервер не проверяет подлинность информации, которую он получает от других серверов.

Таким образом, локальный DNS-сервер не защищен от атак, связанных с подменой IP-адреса при разрешении доменных имён. Также можно заметить, что данные не шифруется, то есть нет настроек DNSoverTLS или DNSoverHTTPS.

# Выводы

В результате выполнения данной работы был изучен формат сообщений и содержимое флагов DNS-ответов.

На основе значений флагов DNS-пакетов был проанализирован локальный DNS-сервер, после чего были сделаны выводы об уровне его защищенности.