Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.03.01 Информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Панин Данила Олегович Группа: 241-351

Место прохождения практики: Московский Политех, кафедра Информационная безопасность

Отчет принят с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель практики: Гневшев Александр Юрьевич

Москва 2025

Содержание

[Введение 3](#_Toc198757113)

[1. Общая информация о проекте 4](#_Toc198757114)

[1.1 Название и обоснование проекта 4](#_Toc198757115)

[1.2 Цель и задачи проекта 4](#_Toc198757116)

[1.3 Ключевые участники проекта 5](#_Toc198757117)

[1.4 Основные функциональные требования 5](#_Toc198757118)

[1.5 Интересы стейкхоллдеров проекта 6](#_Toc198757119)

[1.6 Пути дальнейшего развития 6](#_Toc198757120)

[2. Общая характеристика деятельности организации (заказчика проекта) 8](#_Toc198757121)

[2.1 Наименование заказчика 8](#_Toc198757122)

[2.2 Организационная структура 8](#_Toc198757123)

[2.3 Описание деятельности 8](#_Toc198757124)

[3. Описание задания по проектной практике 9](#_Toc198757125)

[3.1 Разбор инцидента информационной безопасности 9](#_Toc198757126)

[3.2 Базовая часть задания 9](#_Toc198757127)

[3.3 Вариативная часть задания 10](#_Toc198757128)

[4. Описание достигнутых результатов по проектной практике 11](#_Toc198757129)

[4.1 Разбор реального инцидента Midnight Blizzard (2023–2024) 11](#_Toc198757130)

[4.1.1 Особенности и значимость атаки 14](#_Toc198757131)

[4.1.2 Анализ по MITRE ATT&CK: тактики, техники, процедуры 15](#_Toc198757132)

[4.1.3 Вывод по инциденту 16](#_Toc198757133)

[4.2 Базовое задание 17](#_Toc198757134)

[4.2.1 Настройка Git и репозитория 17](#_Toc198757135)

[4.2.2 Подготовка документов в формате Markdown 18](#_Toc198757136)

[4.2.3 Статический веб-сайт 19](#_Toc198757137)

[4.2.4 Взаимодействие с организацией-партнером 30](#_Toc198757138)

[4.3 Вариативная часть задания 33](#_Toc198757139)

[4.3.1 Введение в Вариативное задание 33](#_Toc198757140)

[4.3.2 Аналитическая часть 34](#_Toc198757141)

[4.3.3 Практическая часть 38](#_Toc198757142)

[4.4 Личный вклад в проектную (учебную) практику и распределение времени 75](#_Toc198757143)

[Заключение 77](#_Toc198757144)

[Список использованных источников 79](#_Toc198757145)

# Введение

Настоящий отчёт подготовлен по итогам прохождения проектной (учебной) практики студентами направления «Информационная безопасность» Московского Политехнического университета во втором семестре 2025 года. Практика проводилась в рамках дисциплины «Проектная практика» и включала в себя как индивидуальные, так и групповые задания.

В ходе практики были реализованы следующие этапы:

Знакомство с задачами проектной деятельности и разработка статического веб-сайта, посвящённого командному проекту по теме водных видов спорта.

Взаимодействие с куратором и участие в мероприятии, организованном партнёрской организацией — Московским Политехом.

Выполнение вариативной части задания, заключающейся в реализации методики внешней разведки корпоративной сети, включающей поиск уязвимостей, сбор открытой информации и анализ инфраструктуры.

Практика позволила получить и закрепить навыки командной работы, веб-разработки, работы с системой контроля версий Git, генераторами статических сайтов, а также основам анализа угроз информационной безопасности.

# 1. Общая информация о проекте

## 1.1 Название и обоснование проекта

Название проекта: Водный спорт (I курс).  
Проект был инициирован в рамках дисциплины «Проектная деятельность» с целью разработки информационного ресурса для любителей водных видов спорта. Актуальность проекта обусловлена отсутствием удобной, специализированной платформы, объединяющей информацию о местах (спотах) для занятий такими активностями, как плавание, парусный спорт, водные виды спорта с веслом и моторные виды спорта. Проект также нацелен на повышение интереса к активному образу жизни и поддержку спортсменов, тренеров и новичков через единую цифровую экосистему.

## 1.2 Цель и задачи проекта

**Цель проекта** — создать веб-платформу GoSpot для отображения, фильтрации и оценки мест для водных видов спорта, а также реализовать инструменты взаимодействия между участниками сообщества.

Задачи проекта:

* разработать структуру и контент сайта;
* реализовать сбор и обработку данных о спотах (через парсинг);
* внедрить фильтры по видам спорта и регионам;
* создать систему отзывов и рейтингов;
* организовать хранение данных в структурированном виде;
* интегрировать визуальные элементы и пользовательский интерфейс;
* реализовать разделы сайта: о проекте, участники, журнал, ресурсы, вариативное задание и посещённое мероприятие.

## 1.3 Ключевые участники проекта

* З**аказчиком** проекта выступает Московский Политехнический университет, реализующий учебную дисциплину «Проектная деятельность» для студентов разных направлений.
* **Куратором** проекта является Лебедев Иван Николаевич — преподаватель Московского Политеха, ответственный за сопровождение проектной и учебной деятельности студентов.
* **Функциональные заказчики** (пользователи результатов проекта) — студенты и преподаватели, задействованные в реализации студенческих проектов, а также энтузиасты водных видов спорта, которые будут использовать платформу GoSpot для поиска и оценки локаций.

## 1.4 Основные функциональные требования

* Интерактивная карта с возможностью фильтрации спотов по категориям и регионам.
* Отображение карточек мест с контактной информацией, рейтингом и возможностью оставить отзыв.
* Администрируемое наполнение сайта с возможностью расширения базы данных.
* Реализация отзывчивого и адаптивного интерфейса на базе генератора статических сайтов Hugo.
* Использование собственных стилей CSS и кастомных HTML-шаблонов.

## 1.5 Интересы стейкхоллдеров проекта

* Пользователи (спортсмены, любители, тренеры) — удобный поиск локаций, навигация и отзывы.
* Организации и клубы — возможность продвигать свои споты и мероприятия.
* Образовательное учреждение — развитие компетенций студентов, демонстрация успешных кейсов.
* Команда проекта — получение реального опыта веб-разработки, анализа данных и защиты информации.

## 1.6 Пути дальнейшего развития

* Реализация системы авторизации и пользовательских кабинетов.
* Разработка мобильной версии проекта.
* Интеграция с внешними API (например, Яндекс.Карты, Google Maps) для автоматического обновления информации.
* Поддержка и модерация пользовательского контента.
* Добавление системы мероприятий и бронирования.
* Выход на международный уровень и локализация интерфейса.

# 2. Общая характеристика деятельности организации (заказчика проекта)

## 2.1 Наименование заказчика

Заказчик: ООО “Институт управления имуществом”.

## 2.2 Организационная структура

Организационная структура отсутствует, поскольку структура формируется под конкретные проекты.

## 2.3 Описание деятельности

Осуществляет консультационные и информационные услуги

# 3. Описание задания по проектной практике

Проектная (учебная) практика включала выполнение двух взаимосвязанных частей: обязательной (базовой) и вариативной, а также разбор актуального киберинцидента. Задания были направлены на развитие технических и аналитических навыков студентов, а также на освоение инструментов командной и исследовательской деятельности в области информационной безопасности.

## 3.1 Разбор инцидента информационной безопасности

В рамках аналитической части практики студентам предлагалось изучить один из реальных киберинцидентов, имевших широкую огласку. Задание предполагало:

* поиск и систематизацию информации о хронологии и методах атаки;
* анализ особенностей инцидента с позиции актуальных угроз;
* построение тактик и техник на основе MITRE ATT&CK;
* формирование краткого вывода по значимости инцидента для сферы информационной безопасности.

Результаты работы оформлялись в виде структурированного отчёта, содержащего описание инцидента, применённые методы атаки, таблицу с тактиками и техниками, а также аналитические выводы.

## 3.2 Базовая часть задания

Базовая часть практики предусматривала:

* настройку репозитория в системе контроля версий (GitHub или GitVerse) с использованием шаблона;
* освоение базовых команд Git: клонирование, коммит, пуш, создание веток, написание осмысленных сообщений;
* оформление проектной документации в формате Markdown (описание проекта, журнал, отчёты и др.);
* создание и публикацию статического веб-сайта, включающего:
  + домашнюю страницу с аннотацией;
  + страницу «О проекте» с деталями;
  + вкладку «Участники»;
  + «Журнал» с фиксацией этапов работы;
  + страницу «Ресурсы»;
  + вкладки по вариативному заданию и мероприятию;
* настройку визуального оформления, добавление графики, элементов дизайна и публикацию сайта через GitHub Pages.

## 3.3 Вариативная часть задания

Вариативное задание, выданное кафедрой, касалось **методики внешней разведки корпоративной сети**. В рамках него требовалось:

* настроить окружение и инструменты разведки (Shodan, Amass, Nmap и др.);
* выполнить практическое сканирование и сбор открытой информации;
* систематизировать и представить результаты в виде таблиц, скриншотов и аналитических блоков;
* подготовить отчёт о выполненной работе и интегрировать его в основной сайт проекта.

# 4. Описание достигнутых результатов по проектной практике

## 4.1 Разбор реального инцидента Midnight Blizzard (2023–2024)

В период с ноября 2023 года по январь 2024 года компания **Microsoft** подверглась одной из самых серьёзных кибератак последних лет. Атака была проведена продвинутой государственно поддерживаемой хакерской группировкой **Midnight Blizzard** (также известной как **NOBELIUM** или **APT29**), которая связывается с Службой внешней разведки Российской Федерации (СВР). Эта же группа ранее стояла за атакой на компанию **SolarWinds** в 2020 году.

Изначально компрометация началась с того, что злоумышленники провели атаку типа **password spraying**, то есть массовый перебор паролей к учётным записям в облачной инфраструктуре Microsoft. В результате этой атаки им удалось получить доступ к **устаревшей тестовой учётной записи**, которая не была защищена механизмом многофакторной аутентификации (MFA). Данная учетная запись находилась вне основной производственной среды и, по-видимому, использовалась в рамках разработческих или тестовых процессов, но имела доступ к определённым ресурсам.

Получив первичный доступ, атакующие использовали эту точку входа для дальнейшего проникновения в корпоративную среду. Они провели внутреннюю разведку и получили доступ к **электронной почте сотрудников Microsoft**, включая:

* руководителей высшего звена (топ-менеджмент),
* сотрудников отделов безопасности (иб),
* юридических подразделений,
* отдела, взаимодействующего с правительственными структурами.

Также была зафиксирована попытка получить доступ к **исходному коду некоторых продуктов**, однако Microsoft заявила, что **никаких признаков компрометации клиентских данных** или сервисов (таких как Azure, Outlook, Microsoft 365) обнаружено не было.

Атака оставалась **незамеченной в течение нескольких недель**. Только **12 января 2024 года** специалисты Microsoft обнаружили подозрительную активность, связанную с использованием токенов доступа и несанкционированными попытками взаимодействия с внутренними почтовыми системами. В течение суток, **13 января**, доступ злоумышленников был полностью заблокирован, и началось расследование.

Особенностью атаки стало то, что Midnight Blizzard использовала **инфраструктуру Microsoft против самой Microsoft**: используя легитимные (но скомпрометированные) учетные записи и возможности OAuth, злоумышленники незаметно собирали информацию без привлечения внимания средств защиты.

Позже Microsoft сообщила, что Midnight Blizzard также пыталась **добыть и использовать секретные ключи OAuth**, чтобы получить доступ к сервисам в обход стандартных механизмов аутентификации.

Хронология ключевых событий:

* **Ноябрь 2023** — начало атаки через password spraying, компрометация тестовой учетной записи.
* **Декабрь 2023** — активное пребывание в сети, сбор данных из почтовых ящиков.
* **Январь 2024** — обнаружение активности, блокировка злоумышленников, начало расследования.
* **Февраль–март 2024** — публикация отчётов и усиление защитных мер.

Атака имела серьёзные последствия не только для Microsoft, но и для всей отрасли: она показала, что даже крупные технологические гиганты с развитой системой безопасности могут быть уязвимы при наличии организационных недочётов — в частности, наличия незащищённых тестовых учётных записей и недостаточного контроля за внутренним доступом.

По итогам инцидента Microsoft:

* удалила устаревшие учетные записи без MFA,
* усилила внутреннюю сегментацию и контроль прав доступа,
* пересмотрела политики безопасности токенов и OAuth,
* усилила контроль за внутренней почтовой инфраструктурой,
* ввела дополнительные меры мониторинга и реагирования на подозрительную активность.

### 4.1.1 Особенности и значимость атаки

* **Целью атаки** не были клиенты Microsoft, а именно **внутренняя инфраструктура компании** и её сотрудники.
* Атакующие использовали **password spraying** — перебор паролей к учетным записям без MFA.
* Доступ был получен через **устаревшую тестовую учетную запись**, что подчёркивает важность контроля за "ненужными" пользователями и аккаунтами.
* Midnight Blizzard действовала скрытно в течение **нескольких недель**, прежде чем была обнаружена, что указывает на высокий уровень подготовки.
* Был использован **собственный инфраструктурный доступ Microsoft** — атака затронула доверенные внутренние системы.

### 4.1.2 Анализ по MITRE ATT&CK: тактики, техники, процедуры

**Таблица 1 Тактики и техники атаки.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | Тактика (Tactic) | Tactic ID | Техника (Technique) | Technique ID | Применение в атаке Midnight  Blizzard |
| **1** | Initial Access (первичный доступ) | TA0001 | Password Spraying | T1110.003 | Атакующие перебирали пароли для входа в облачные сервисы Microsoft и получили доступ к тестовой учётной записи без MFA. |
| **2** | Credential Access  (доступ к учетным данным) | TA0006 | Valid Accounts | T1078 | Злоумышленники использовали действующую учётную запись для доступа к внутренней инфраструктуре. |
| **3** | Persistence (удержание в системе) | TA0003 | Create Account | T1136 | Были созданы новые учётные записи для поддержания доступа. |
| **4** | Defense Evasion (обход защиты) | TA0005 | Impair Defenses | T1562.001 | Использовались легитимные токены и внутренние механизмы Microsoft для обхода стандартных средств защиты. |
| **5** | Discovery (разведка в системе) | TA0007 | Remote  System  Discovery | T1018 | Проводился анализ внутренней сетевой инфраструктуры и доступных сервисов. |
| **6** | Collection (сбор информации) | TA0009 | Email Collection | T1114 | Были собраны письма топменеджеров и сотрудников отделов безопасности и юристов. |
| **7** | Exfiltration  (эксфильтрация данных) | TA0010 | Exfiltration  Over C2  Channel | T1041 | Вывод данных через удалённые каналы управления без генерации тревог. |

### 4.1.3 Вывод по инциденту

Атака Midnight Blizzard стала одним из наиболее заметных и опасных инцидентов за последние годы. Она продемонстрировала:

* важность контроля даже над **вспомогательными учетными записями** (тестовые, архивные);
* **недостаточность одного пароля** как средства защиты — даже в крупной корпорации;
* необходимость **внедрения и строгого применения многофакторной аутентификации (MFA)** для всех пользователей;
* высокий уровень подготовки и скрытности действий злоумышленников, типичный для государственно поддерживаемых APT-групп;
* актуальность поведенческого анализа (по моделям MITRE ATT&CK) при расследовании сложных атак.

Изучение данного инцидента позволяет понять, как даже хорошо защищённая организация может стать жертвой при недооценке базовых мер безопасности.

## 4.2 Базовое задание

### 4.2.1 Настройка Git и репозитория

На начальном этапе практики было выполнено задание по созданию и настройке репозитория для хранения исходных файлов проекта. В соответствии с методическими рекомендациями, на платформе GitHub был создан групповой репозиторий по адресу:

<https://github.com/stepanstoliarzh/practice-2025-Stoliarzh-Panin-Boykov>

Работа с Git осуществлялась преимущественно через терминал Git Bash. Были освоены и активно применялись базовые команды: git clone, git commit, git push, git pull, git checkout, git branch. Особое внимание уделялось практике осмысленного оформления сообщений коммитов для удобной командной работы и отслеживания изменений.

Команда организовала работу в двух ветках, так как в основной ветке сайт не удавалось запустить(решение проблемы не было найдено).

### 4.2.2 Подготовка документов в формате Markdown

Для документационного сопровождения проекта были подготовлены и оформлены файлы в формате Markdown. Основными документами стали:

* README.md во многих папках проекта, с описанием раздела;
* ВзаимодействиеСПартнером .md — отчёт о посещении Дня открытых дверей;
* ОтчетобВариативномЗадании.md — подробный отчёт о выполнении вариативной части задания;
* Документация.md — описание этапов выполнения практики;

Для освоения синтаксиса Markdown использовались официальные материалы GitHub и документация Hugo. Были изучены базовые конструкции:

заголовки, списки, таблицы, изображения, ссылки и форматирование текста.

Файлы редактировались вручную в текстовом редакторе VS Code с установленным предпросмотром Markdown.

### 4.2.3 Статический веб-сайт

#### 4.2.3.1 Инициализация проекта

27 апреля 2025 года изначально было принято решение реализовать сайт вручную, используя базовые технологии HTML и CSS. Однако после первых попыток стало очевидно, что ручная сборка затруднительна в поддержке, плохо масштабируется и требует гораздо больше времени на реализацию навигации и стилизации. К 29 апреля было принято решение перейти на использование генератора статических сайтов **Hugo**, так как он обеспечивает высокую скорость разработки, удобную структуру проекта, а также наличие широкого выбора тем и встроенную поддержку Markdown.

#### 4.2.3.2 Выбор и настройка темы

29 апреля мы выбрали тему **Blowfish**, мотивируя это её

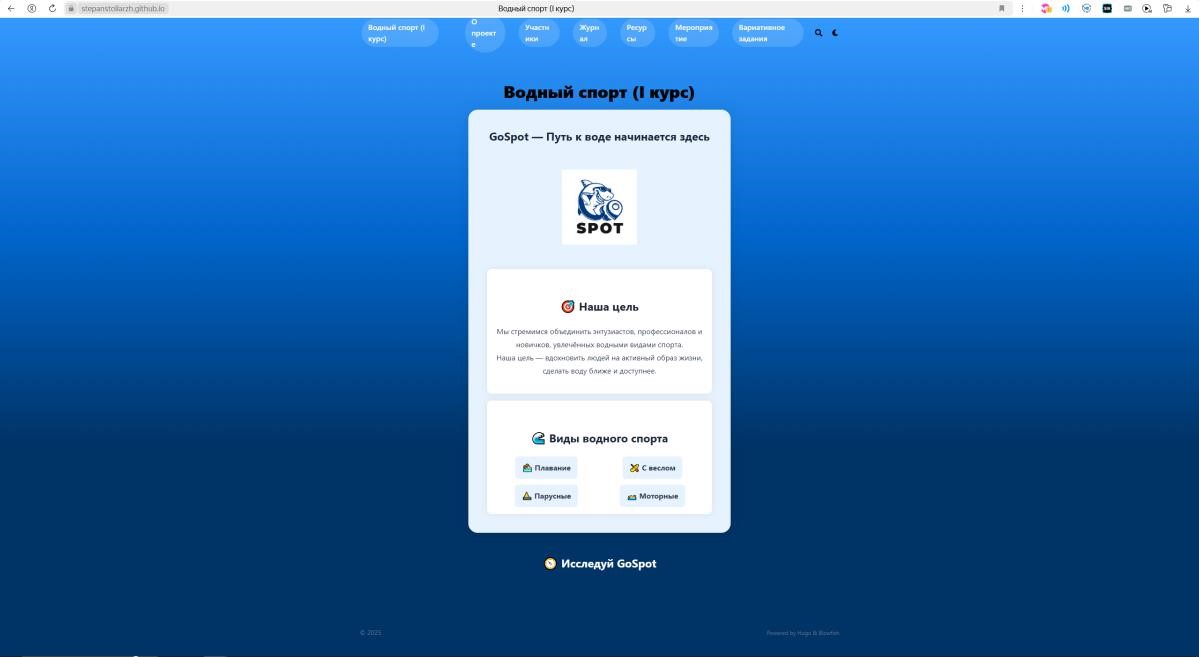
минималистичным дизайном, гибкостью настройки и ассоциативной связью с водной тематикой, что косвенно отражает направленность проекта «Водный спорт». Тема была успешно подключена, после чего были выполнены базовые настройки стилей, шапки и структуры меню.

#### 4.2.3.3 Создание разделов

С 7 апреля по 17 мая производилось создание и наполнение информацией следующих страниц:

* Домашняя страница:

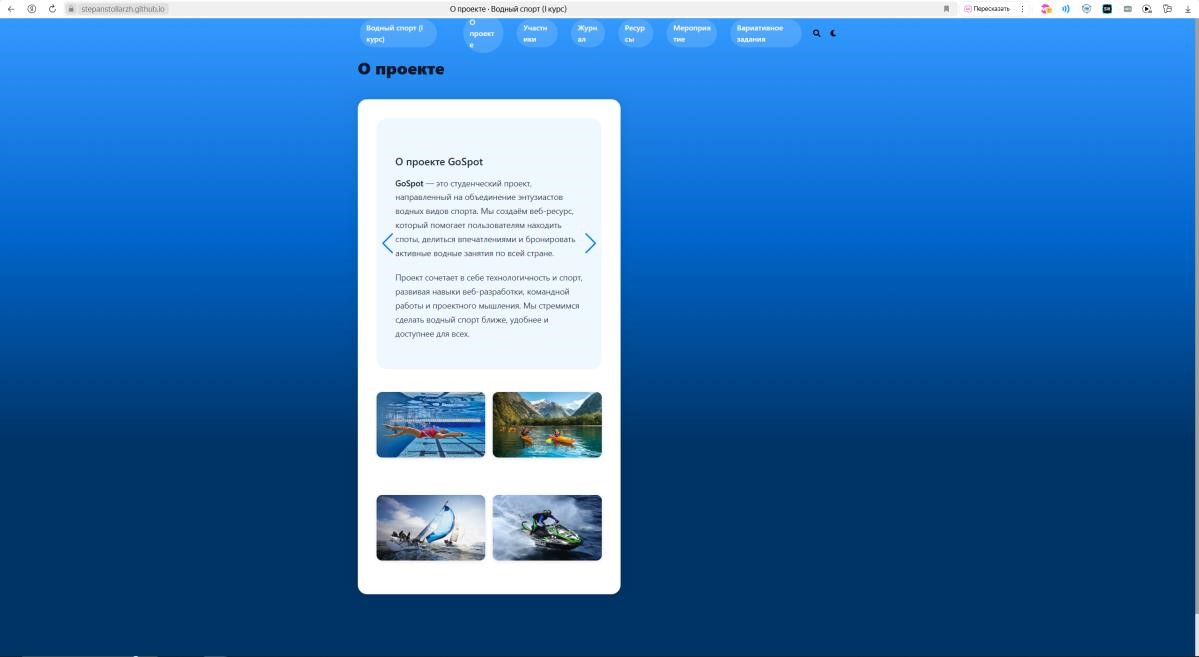
Содержит краткую аннотацию проекта, его цели и задачи (*см. Рис 1*). Является стартовой точкой навигации, откуда можно перейти ко всем остальным разделам сайта.



*Рис 1 Вкладка Домашняя страница*

* О проекте:

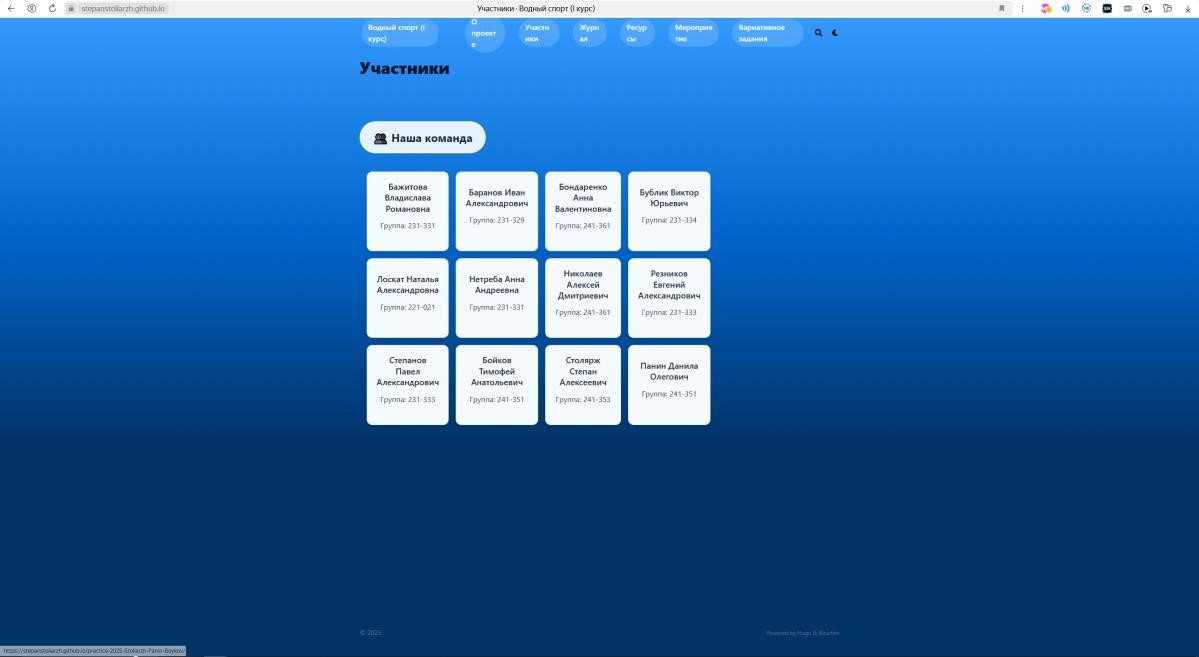
Раздел, посвящённый подробному описанию проекта, его миссии, структуре, используемым технологиям и ключевым участникам разработки (*см.* *Рис 2*).



*Рис 2 Вкладка О проекте*

* Участники:

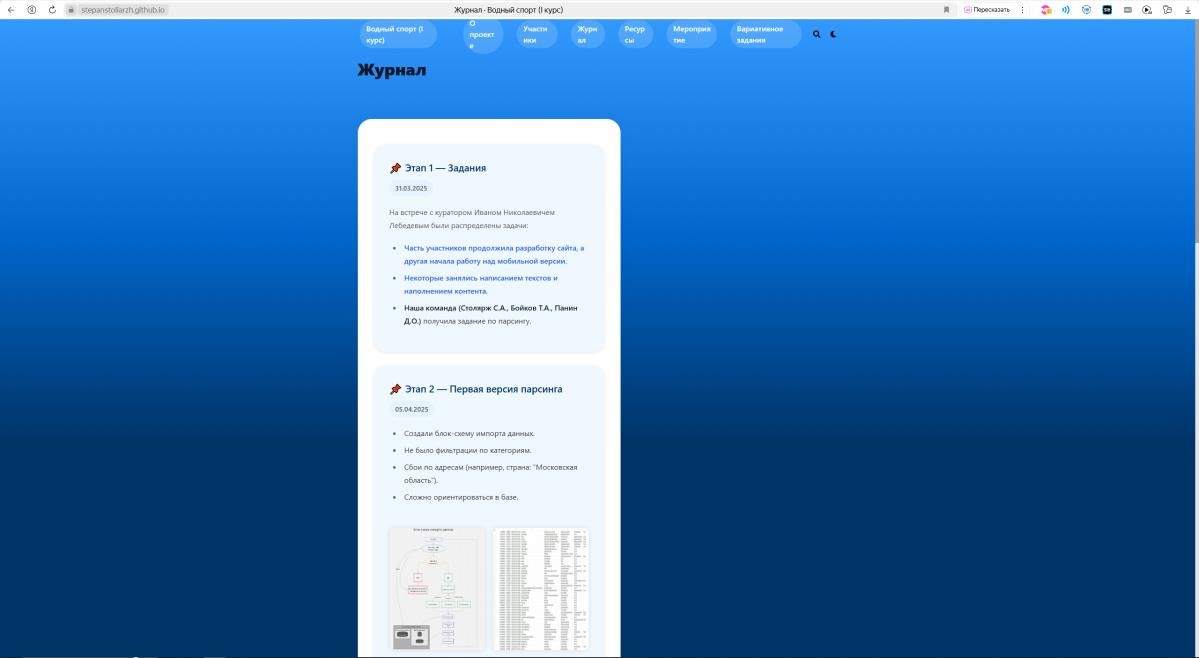
Содержит информацию о составе команды, распределении обязанностей и личном вкладе каждого участника в реализацию проекта (*см. Рис 3*).



*Рис 3 Вкладка Участники*

* Журнал:

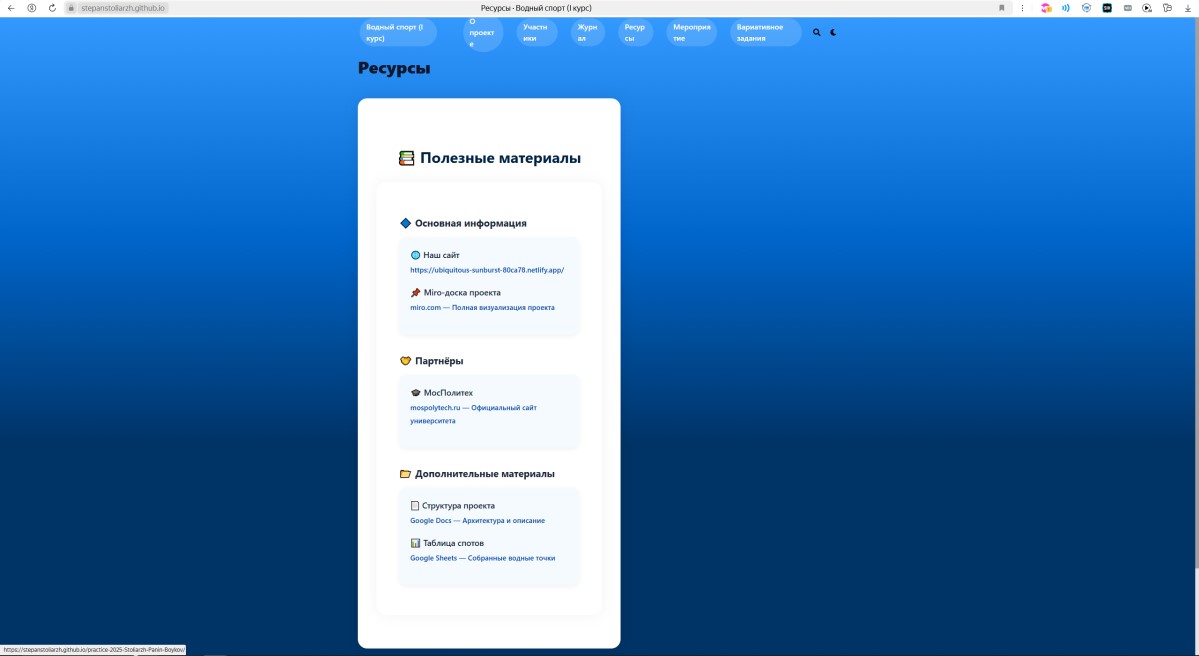
Раздел, в котором поэтапно отражены все этапы выполнения проекта с указанием дат (*см. Рис 4*). Включает краткие отчёты о проделанной работе: распределение задач, создание блок-схемы, реализация фильтрации, добавление международных спотов, улучшение интерфейса и наполнение контентом. Журнал служит хронологией развития проекта и демонстрирует прогресс команды.



*Рис 4 Вкладка Журнал*

* Ресурсы:

На странице представлены полезные материалы, ссылки на использованные инструменты, методические материалы, а также документы, связанные с реализацией проекта (*см. Рис 5*).



*Рис 5 Вкладка Ресурсы*

* Мероприятие:

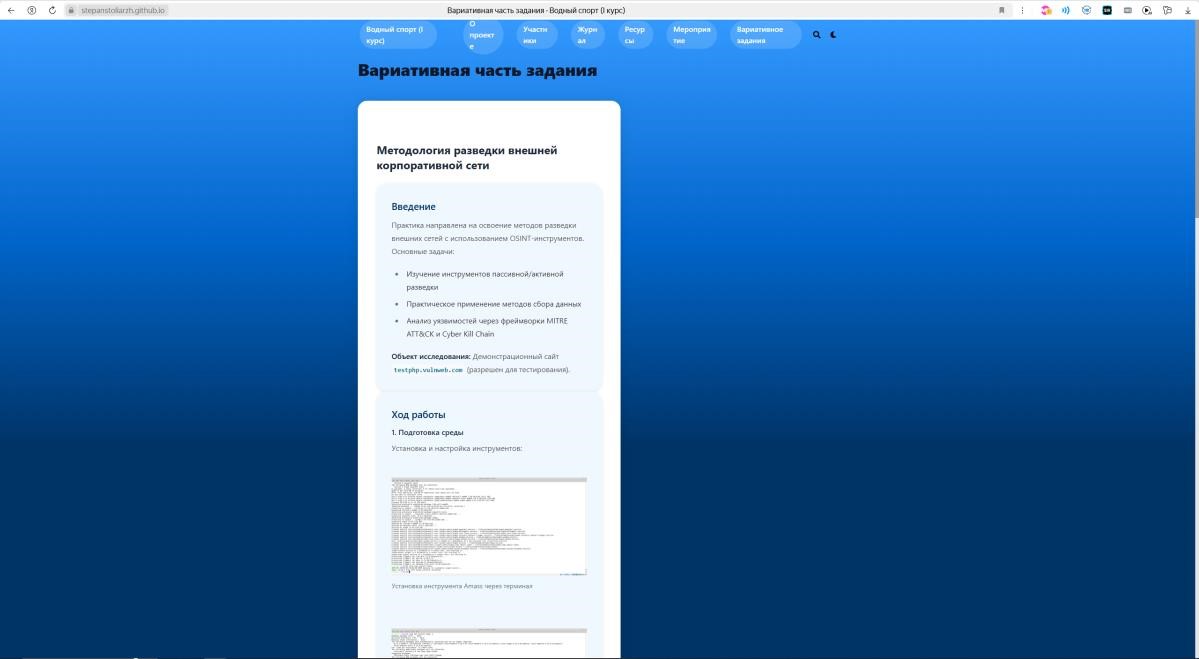
Раздел описывает посещённое мероприятие в рамках проектной практики — День открытых дверей Московского Политеха (*см. Рис 6*). Включает фотоотчёт, впечатления участников и выводы.



*Рис 6 Вкладка Мероприятие*

* Вариативное задание:

Отражает реализацию группового кафедрального задания: «Методика внешней разведки корпоративной сети» (*см. Рис 7*). Представлены этапы работы, использованные инструменты и визуализация результатов.



*Рис 7 Вкладка Вариативное задание*

Относительно длительный срок выполнения связан с тем, что команда пропустила ранние мероприятия, и единственным доступным для посещения стал День открытых дверей 17 мая. Также в этот период проводилось оформление сайта: была разработана собственная стилистика проекта (белый фон, закругленные блоки, оформление карточек), добавлены изображения, иллюстрации и декоративные элементы. Отдельное внимание было уделено мобильной версии: часть CSS-стилей адаптирована под экраны с шириной менее 768 пикселей, что позволило корректно отображать структуру на смартфонах.

#### 4.2.3.4 Публикация

С 17 по 19 мая производились попытки публикации сайта на GitHub Pages. Основной проблемой стало некорректное подключение пользовательских стилей (*см. Рис 8*), в результате чего сайт отображался без оформления. Из-за отсутствия предварительного опыта устранение этой ошибки заняло значительное количество времени. Впоследствии была выявлена проблема с путями к стилям, что было успешно исправлено, и сайт был опубликован в актуальном виде.



*Рис 8 Вкладка Домашняя страница с проблемой подключения стилей*

#### 4.2.3.5 Используемые технологии

**Таблица 2 Инструменты, использованные в разработке**

|  |  |
| --- | --- |
| **Инструмент** | **Назначение** |
| Git, GitHub | Система контроля версий и хостинг проекта |
| HTML, CSS | Разметка и стилизация страниц |
| Markdown | Форматирование текстовых материалов |
| Hugo | Генерация и сборка статического сайта |

#### 4.2.3.6 Вывод о создании сайта

В рамках выполнения проекта были получены практические навыки создания статического сайта с помощью Hugo и базового HTML. Участники освоили структуру проекта Hugo, принципы адаптивной верстки, написание содержимого в формате Markdown, а также групповые методы взаимодействия при отладке публикации. В результате был реализован полноценный сайт с семью основными страницами, оформленный в едином визуальном стиле.

### 4.2.4 Взаимодействие с организацией-партнером

#### 4.2.4.1 День открытых дверей в Московском Политехе, 17.05.2025

В субботу, 17 мая, студенты нашей группы приняли участие в **Дне открытых дверей Московского Политеха** — мероприятии, которое объединило сотни абитуриентов, студентов и преподавателей в стенах главного кампуса.

С первых минут на входе нас встретила приятная атмосфера: баннеры, современная навигация и дружелюбные волонтёры, готовые помочь с любыми вопросами.



*Рис 9 Перед входом и вход в здание Московского Политеха*

*Образовательные стенды и выступления*

Среди множества стендов и презентаций мы уделили особое внимание техническим и IT-направлениям. Преподаватели делились инсайтами по программам, таким как кибербезопасность, разработка ПО и проектная деятельность. Были затронуты темы стажировок, проектов с индустриальными партнёрами и будущих научных мероприятий.

Также нам удалось пообщаться с организаторами проектной практики, где мы узнали, как можно применить наши знания по информационной безопасности в рамках междисциплинарных кейсов.



*Рис 10 Наша команда*

*Раздаточные материалы и впечатления*

Каждому участнику мероприятия вручили красочную брошюру с подробным описанием факультетов, направлений и студенческой жизни. Внутри содержалась информация о бакалавриате, специалитете и магистратуре, а также советы по адаптации для первокурсников.



*Рис 11 Брошура, пенал и ручка*

Бонусом стали небольшие подарки — стильный пенал и ручки. Такие детали сделали посещение особенно тёплым и запоминающимся.

*Вывод о мероприятии*

Мероприятие позволило нам по-новому взглянуть на наш университет. Несмотря на то, что мы уже являемся студентами Политеха, **День открытых дверей стал возможностью расширить кругозор, увидеть “изнанку” организации образовательного процесса и почувствовать себя частью большого сообщества**.

## 4.3 Вариативная часть задания

### 4.3.1 Введение в Вариативное задание

Учебная практика по теме «Методология разведки внешней корпоративной сети», включает в себя изучение методов и инструментов разведки, применяемых в процессе оценки защищенности информационных систем. Практика основана на анализе открытых источников и практическом применении инструментов OSINT и активной разведки.

Цель учебной практики — получить теоретические знания и практические навыки в области разведки информации, освоить методы сбора и анализа данных об информационных системах, а также научиться применять полученные знания для выявления потенциальных уязвимостей.

Для достижения поставленной цели были решены следующие задачи:

1. Изучение теоретических основ разведки в информационной безопасности.
2. Анализ методов и инструментов пассивной и активной разведки.
3. Изучение технической документации и практических руководств по применению инструментов разведки.
4. Проведение практических упражнений по сбору информации с использованием различных инструментов.
5. Подготовка отчета о проделанной работе с анализом полученных данных.

Объектом исследования является методология разведки в информационной безопасности.

### 4.3.2 Аналитическая часть

#### 4.3.2.1 Общая информация о разведка

Разведка (Reconnaissance) в контексте информационной безопасности — это процесс сбора информации о целевой системе или организации с целью выявления потенциальных уязвимостей. Разведка делится на два основных типа:

* Пассивная разведка: сбор информации без прямого взаимодействия с целью, например, анализ открытых источников, поиск в базах данных утечек, изучение метаданных файлов.
* Активная разведка: сбор информации с прямым взаимодействием с целью, например, сканирование портов, перебор директорий, анализ сетевого трафика.

#### 4.3.2.2 Инструменты развелки

1. whois — утилита для запроса WHOIS-протокола, возвращающая информацию о регистрации домена или IP-адреса (регистратор, даты регистрации/истечения, контактные данные)
2. Amass / sublist3r — сбор поддоменов и построение графа «attack surface» с пассивными и активными методами
3. Shodan / Censys — поиск устройств и сервисов по баннерам, мониторинг «живой» экспозиции внешней поверхности сети
4. Nmap — сканер портов и сервисов с NSE-скриптами для баннерграббинга и fingerprinting-а ОС
5. Masscan — очень быстрое сканирование больших IP-диапазонов, альтернатива Nmap для простого port-sweep
6. theHarvester — сбор email-адресов, поддоменов и упоминаний из поисковых систем и публичных баз
7. Dirsearch / FFUF — brute-force скрытых директорий и файлов на веб-сервере.
8. WhatWeb / HTTPX — fingerprinting веб-технологий, определение CMS и WAF
9. Nuclei / OpenVAS — шаблонное сканирование уязвимостей на основе CVE
10. Recon-ng / Maltego — модульные фреймворки для автоматизации

OSINT-запросов и визуализации связей

1. Python (requests, BeautifulSoup) — платформа для кастомных скриптов: парсинг веб-страниц и интеграция с API
2. LeakIX / crt.sh — мониторинг утечек данных и истории SSL/TLSсертификатов для выявления скрытых субдоменов
3. Hunter.io — поиск и верификация email-структур домена, полезно для сбора контактной информации и планирования фишинговых сценариев

#### 4.3.2.3 Применение фреймворков

Фреймворки в области информационной безопасности предоставляют структурированные подходы к пониманию и анализу действий злоумышленников. Они помогают организациям выявлять, предотвращать и реагировать на киберугрозы.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) (**<https://attack.mitre.org/>**)— это база знаний о тактиках и техниках, используемых злоумышленниками в реальных атаках. Она организована в виде матрицы, где строки представляют тактики (цели злоумышленников), а столбцы — техники (способы достижения целей).

Применение MITRE ATT&CK позволяет:

* Классифицировать и анализировать поведение злоумышленников.
* Разрабатывать и улучшать меры защиты.
* Оценивать эффективность существующих средств безопасности.
* Проводить обучение и тренировки персонала.

Cyber Kill Chain (**<https://www.darktrace.com/cyber-ai-glossary/cyber-kill-chain>**) — это модель, которая описывает этапы кибератаки от первоначальной разведки до достижения целей злоумышленника. Она включает следующие этапы:

1. Разведка (Reconnaissance) — сбор информации о цели.
2. Вооружение (Weaponization) — создание вредоносного ПО.
3. Доставка (Delivery) — передача вредоносного ПО цели.
4. Эксплуатация (Exploitation) — использование уязвимостей для выполнения вредоносного кода.
5. Установка (Installation) — установка вредоносного ПО на целевой системе.
6. Управление (Command and Control) — установление связи с командным сервером.
7. Достижение целей (Actions on Objectives) — выполнение конечных целей атаки, таких как кража данных или разрушение систем.

Модель Cyber Kill Chain помогает организациям выявлять и прерывать атаки на ранних этапах, а также разрабатывать стратегии защиты и реагирования на инциденты.

#### 4.3.2.4 Сравнение и критериев выбора инструментов

**Таблица 3 Критерии выбора инструментов**

|  |  |
| --- | --- |
| **Критерий** | **Что важно учитывать ?** |
| Удобство | CLI/GUI, кроссплатформенность, документация |
| Скорость | Производительность при сканировании диапазонов |
| Точность | Минимум ложных срабатываний, полнота данных |
| Автоматизация | Наличие API и возможность интеграции в пайплайн |
| Обновляемость | Регулярные апдейты и поддержка новых техник |

Был выбран такой набор инструментов:

* Amass – инструмент для сбора поддоменов и построения графов связей.
* Shodan – API-интерфейс для поиска открытых устройств по IP и сервисам.
* nmap –инструмент сетевого сканирования с множеством скриптов NSE.
* Python (requests) – универсальная платформа для кастомных решений.
* LeakIX– для поиска экспозиций и утечек.
* Hunter.io – для выявления email-структур домена.
* whois — утилита, возвращающая информацию о регистрации домена или IPадреса.

### 4.3.3 Практическая часть

#### 4.3.3.1 Обоснование выбора цели исследования

В рамках учебной практики по теме внешней разведки корпоративных сетей крайне важно выбрать корректную и безопасную цель для проведения тестов. Согласно действующему законодательству, сканирование и разведка публичных ресурсов без разрешения их владельцев может нарушать нормы права, в том числе статьи, связанные с несанкционированным доступом и вмешательством в информационные системы. Проведение даже пассивной разведки (например, анализа DNSзаписей, WHOIS-информации или портов) на реальных коммерческих доменах без юридического согласия может считаться неправомерным.

Альтернативой мог бы быть домен example.com, который

официально зарезервирован для демонстрационных и образовательных целей. Однако, данный домен не связан с реальной инфраструктурой: он не имеет активных сервисов, IP-адресов или веб-сайта, что делает практику анализа, разведки и моделирования угроз на его основе бессмысленной с точки зрения обучения.

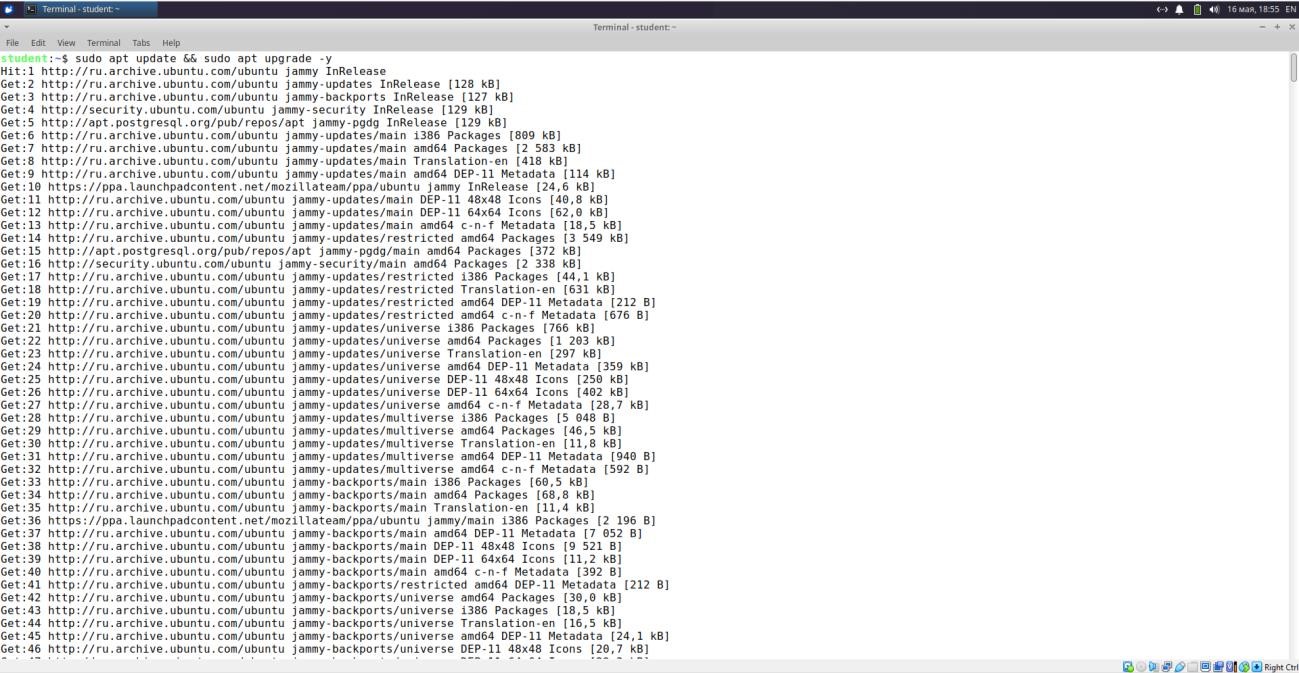
В связи с этим был выбран специальный сайт testphp.vulnweb.com, предоставленный компанией Acunetix — разработчиком инструментария для тестирования безопасности веб-приложений. Этот сайт:

* предназначен специально для учебных целей и оценки уязвимостей,
* заранее уязвим по ряду векторов атак, что делает его полезным для отработки методик разведки,
* официально разрешён для публичного сканирования, в том числе инструментами типа nmap, Amass, Shodan, WHOIS и OSINT-фреймворками.

Таким образом, выбор testphp.vulnweb.com обеспечивает соблюдение правовых норм, позволяет провести реалистичную практику по сбору разведывательных данных, выявлению поверхностных уязвимостей и моделированию действий злоумышленников с опорой на стандарты, такие как MITRE ATT&CK и Cyber Kill Chain. Это делает его идеальной платформой для учебной отработки этапа Reconnaissance в рамках безопасного и этичного пентеста.

#### 4.3.3.2 Проведение разведки

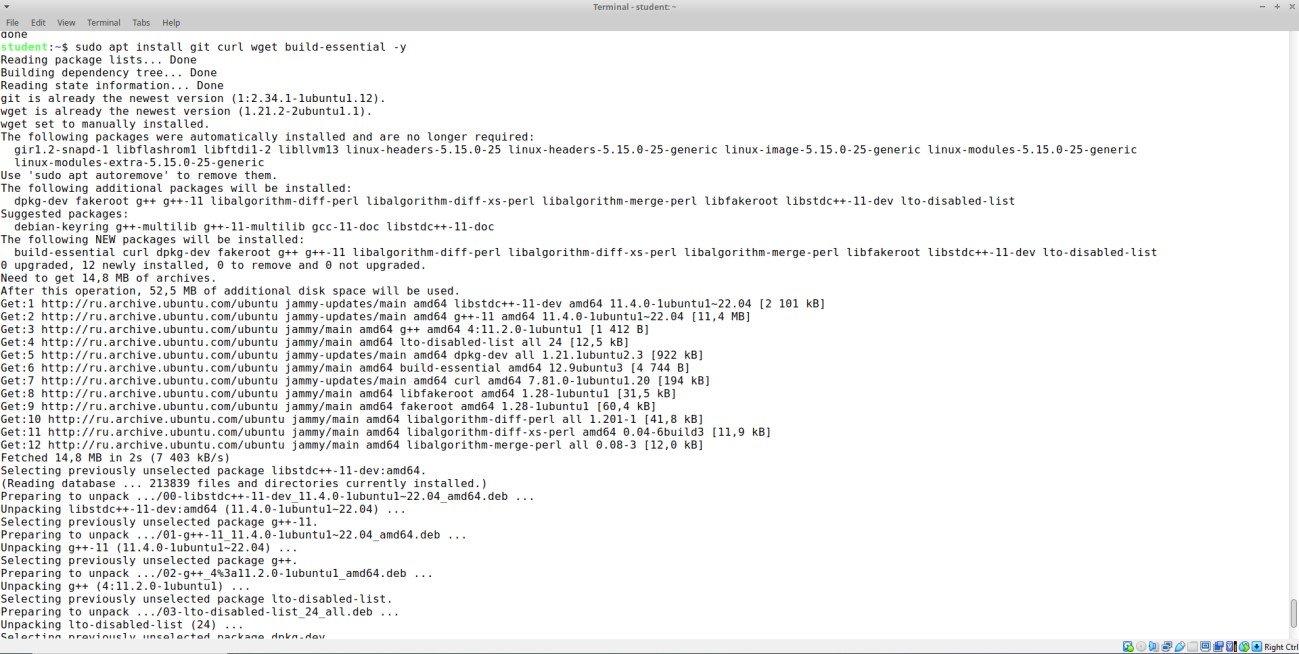
Сначала обновляем систему воспользовавшись командой sudo apt update && sudo apt upgrade -y .



*Рис 12 Обновление системы*

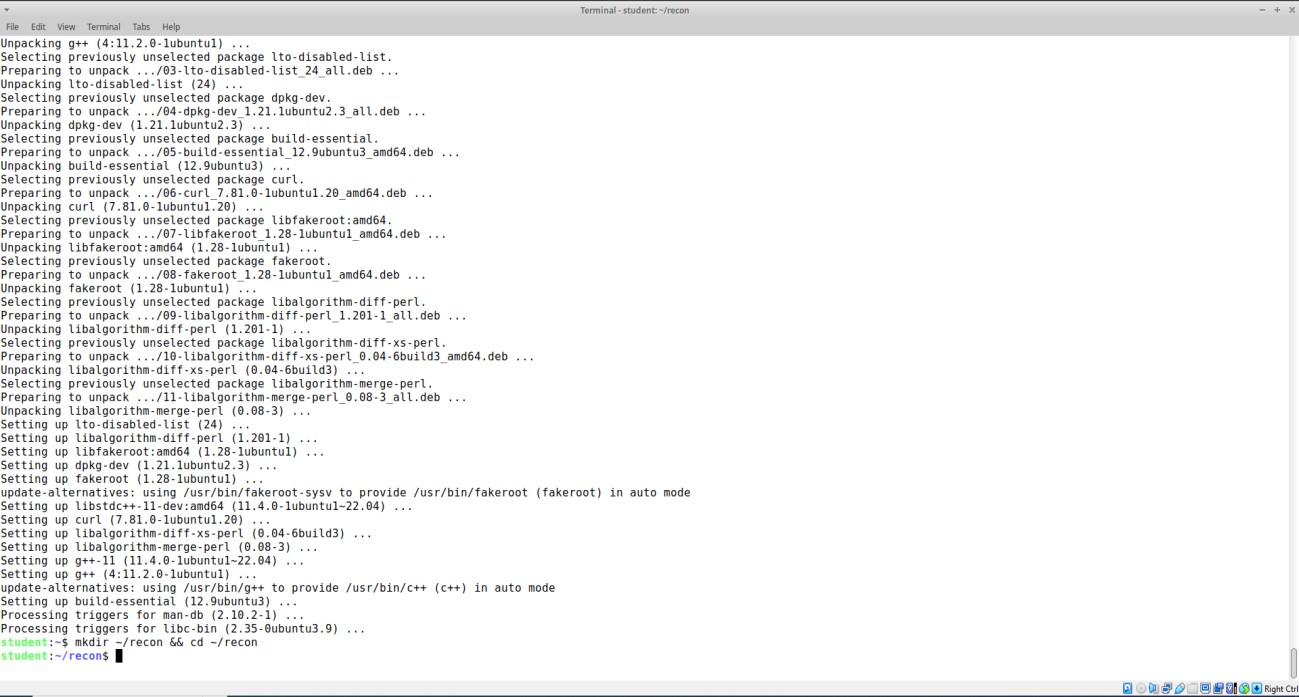
Устанавливаем базовые утилиты с помощью команды “sudo apt install git curl wget build-essential -y”.

* git — система контроля версий, позволяет скачивать и управлять репозиториями кода.
* curl — утилита для отправки HTTP-запросов и скачивания данных с вебсайтов.
* wget — аналог curl, часто используется для скачивания файлов по URL.
* build-essential — набор инструментов для сборки программ из исходного кода (включает компиляторы gcc, g++, make и базовые библиотеки).



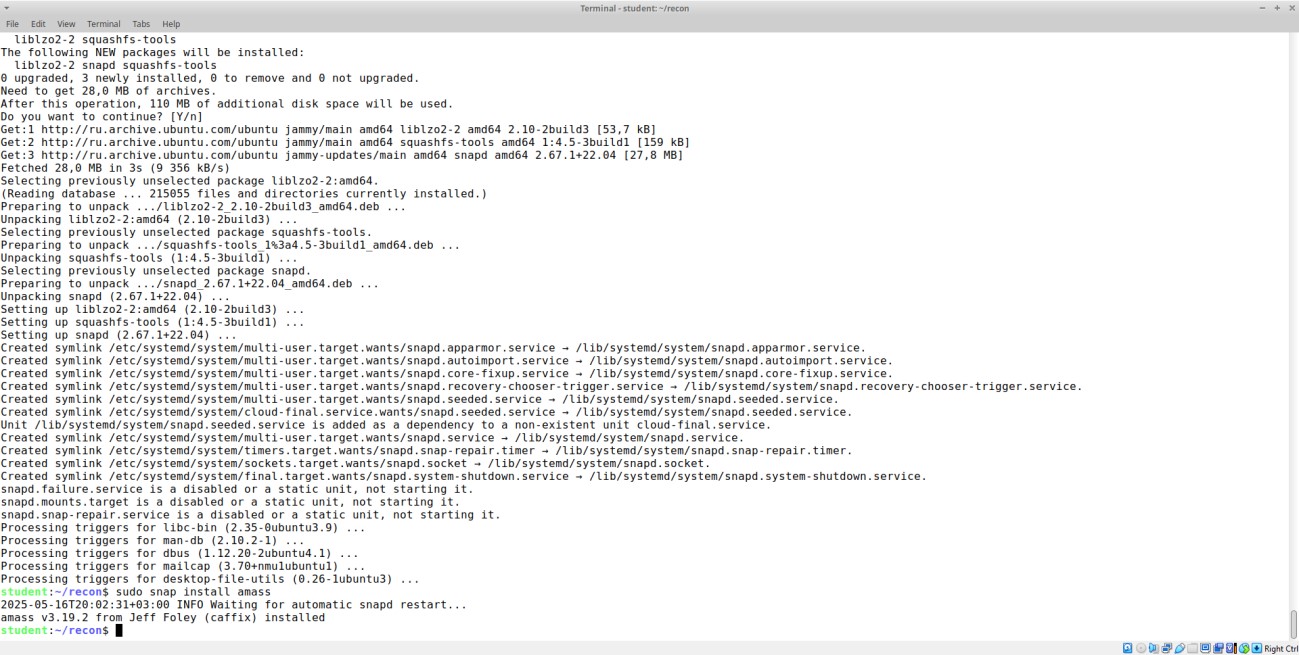
*Рис 13 Установка утилит git curl wget build-essential*

Создайте рабочую директорию, где будут храниться скрипты, результаты и отчёты. Введя команду “mkdir ~/recon && cd ~/recon”.



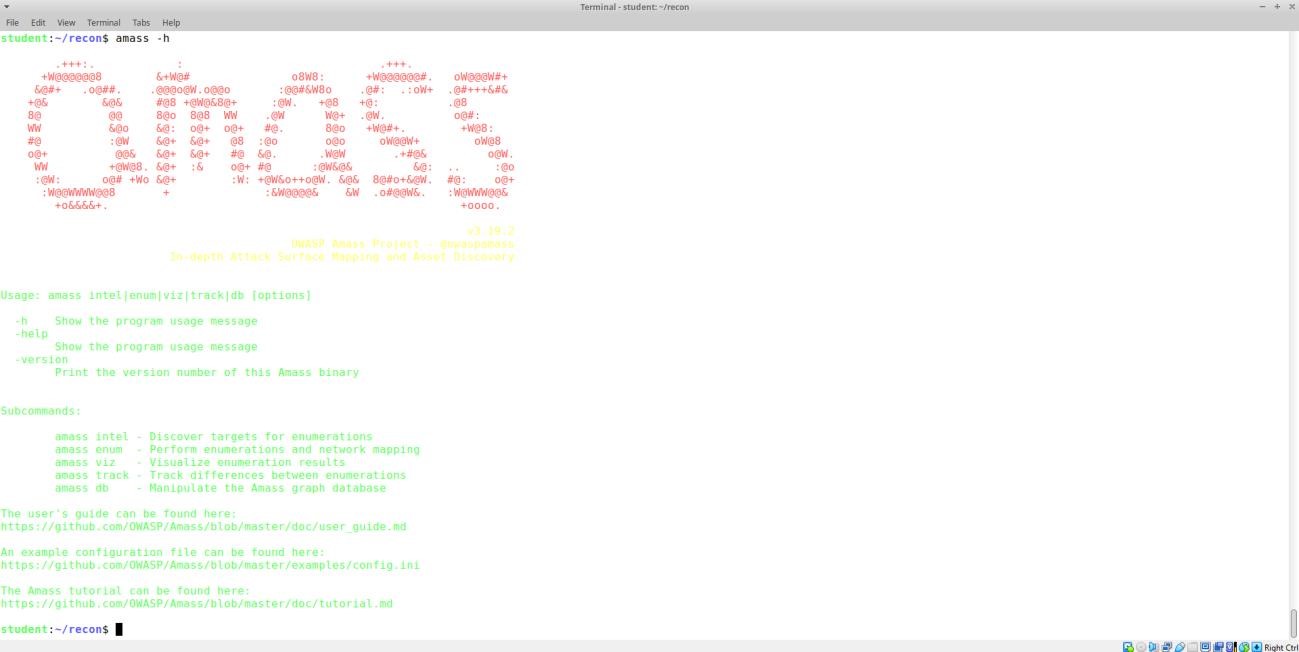
*Рис 14 Создаем директорию*

Устанавливаем amass, с помощью snapd. Используя, “sudo apt install snapd и sudo snap install amass”.



*Рис 15 Установка amass*

Проверяем установку amassa, введя команду amass -h , которая выводит справку по всем глобальным параметрам (например список субкоманд).



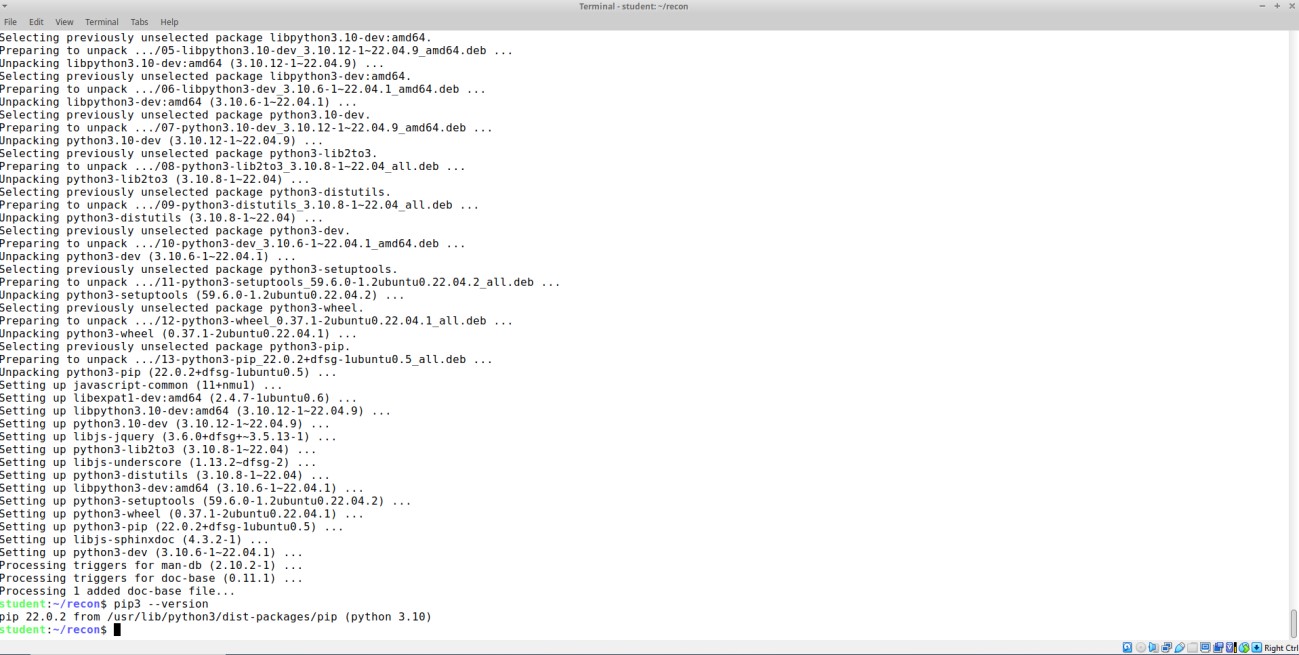
*Рис 16 Проверка amass*

Установка пакет python3-pip, который необходим для установки shodan.



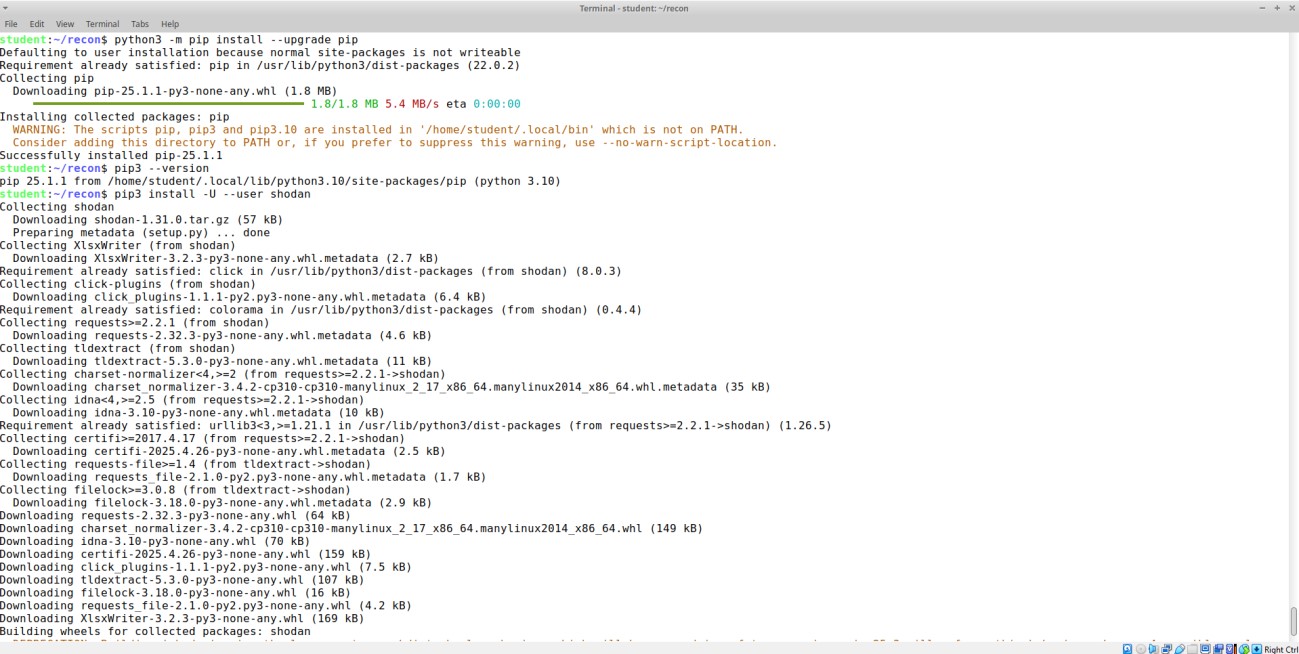
*Рис 17 Установка pip-пакетов*

Проверяем установку pip3-пакета и видим что , установлена не самая новая версия pip-пакетов, их следует обновить.



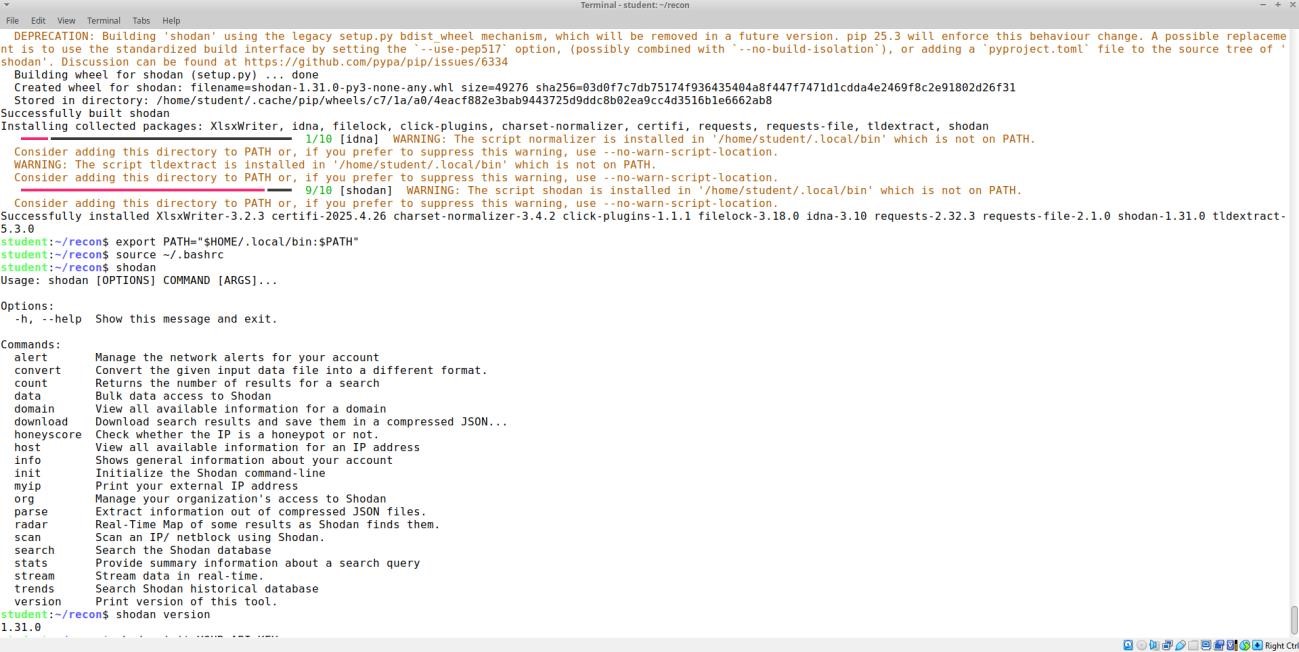
*Рис 18 Проверка pip-пакетов*

Обновляем pip-пакет и начинаем установку shodan.



*Рис 19 Обновление pip-пакетов*

Расширяем системный путь, добавляя в него ~/.local/bin, чтобы оболочка автоматически находила там установленные утилиты.



*Рис 20 Расширение системного пути*

Регистрируемся на сайте shodan для получения api-ключа.

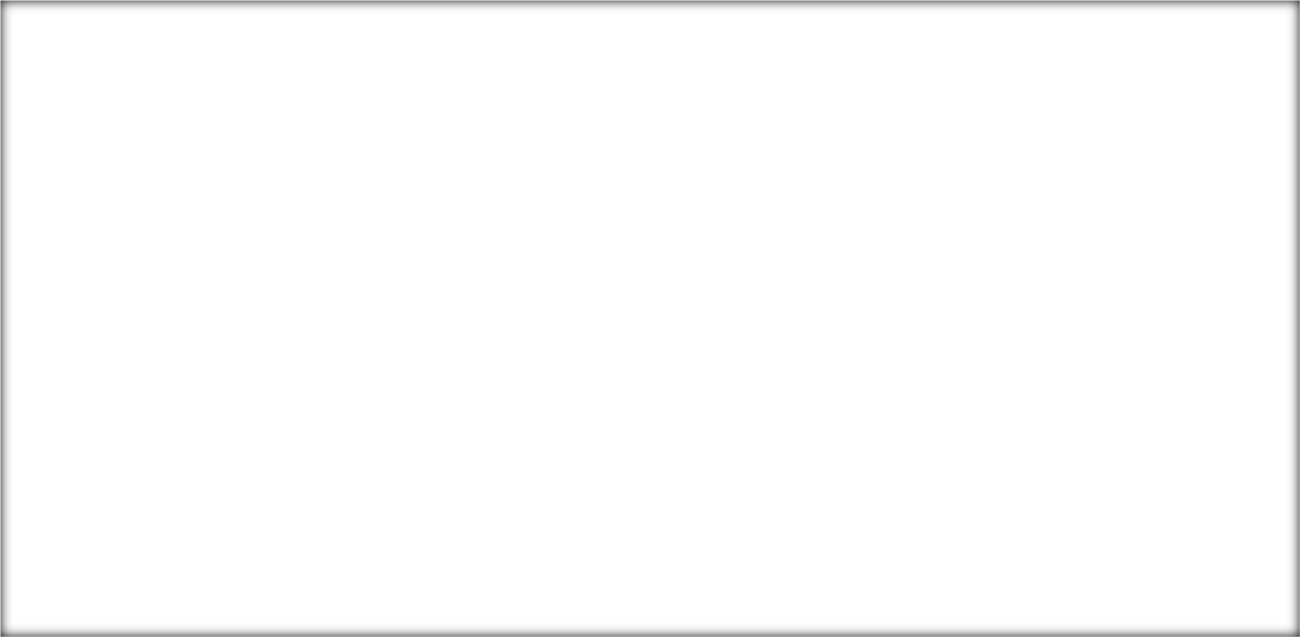
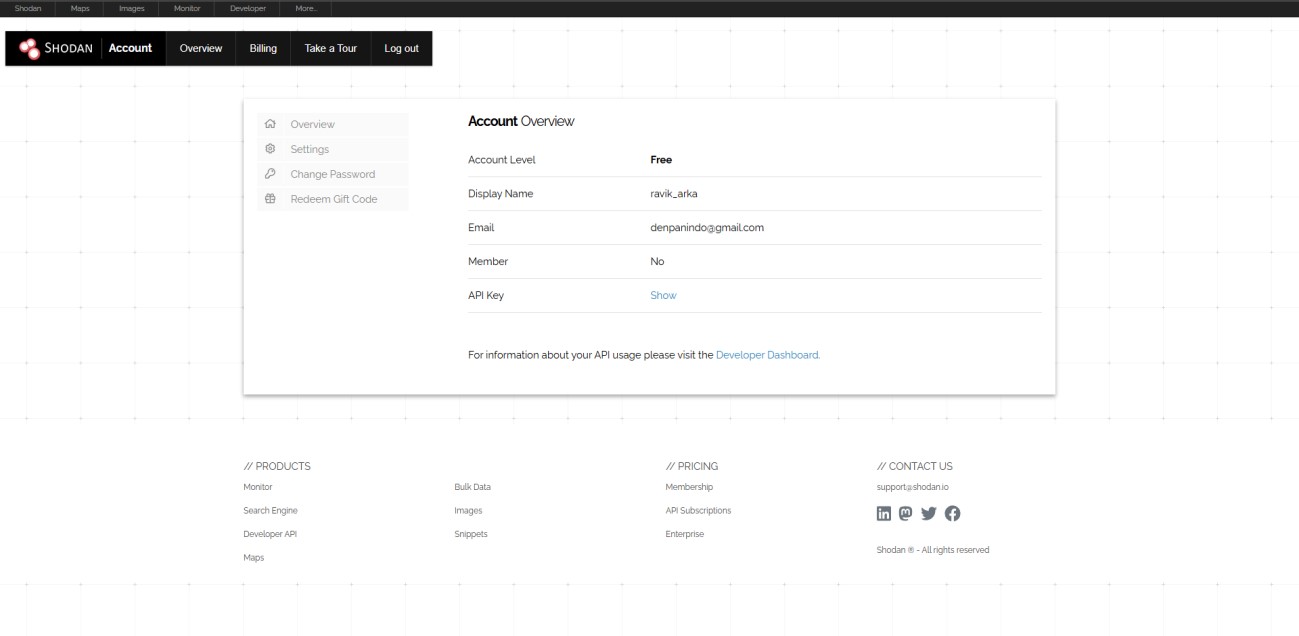
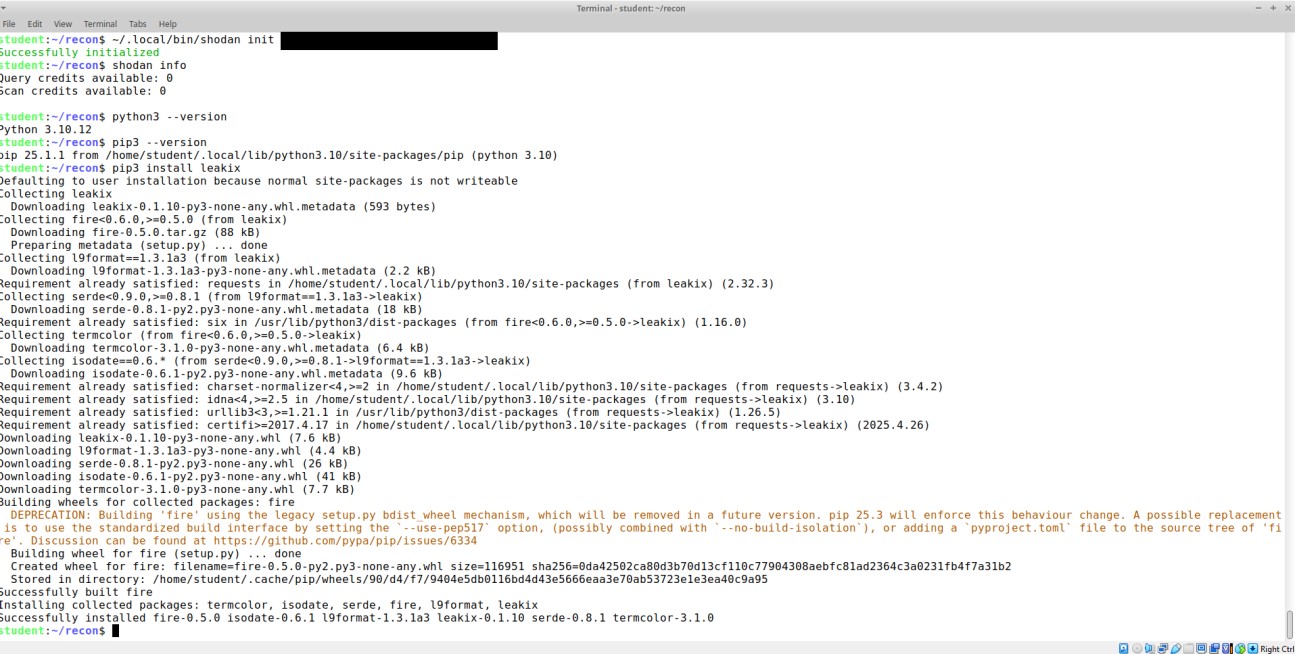


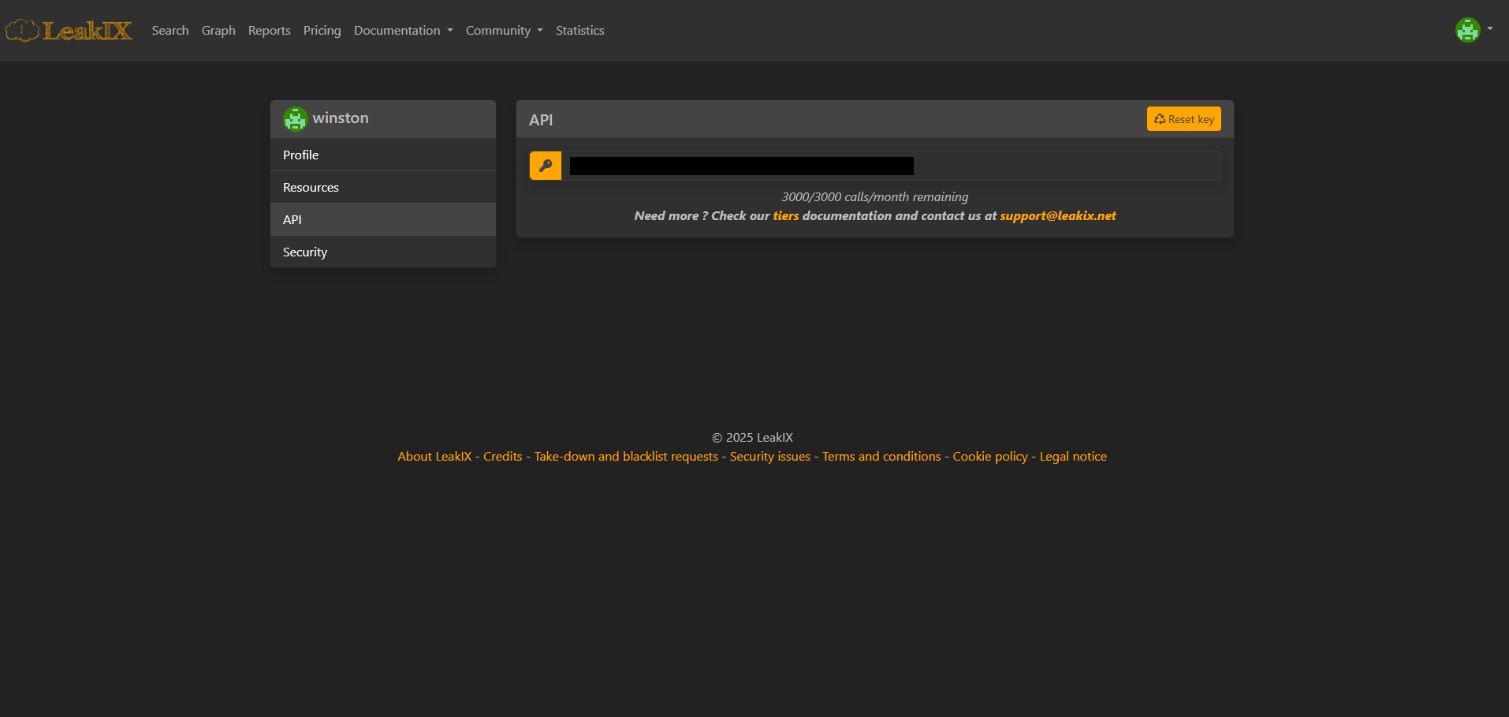
Рис 45 Регистрация на сайте Shodan

Инициализация API-ключа shodan и проверка его работы. После устанавливаем LeakIX Python-клиент(Клиент позволяет обращаться к LeakIX API в формате Python-объектов).



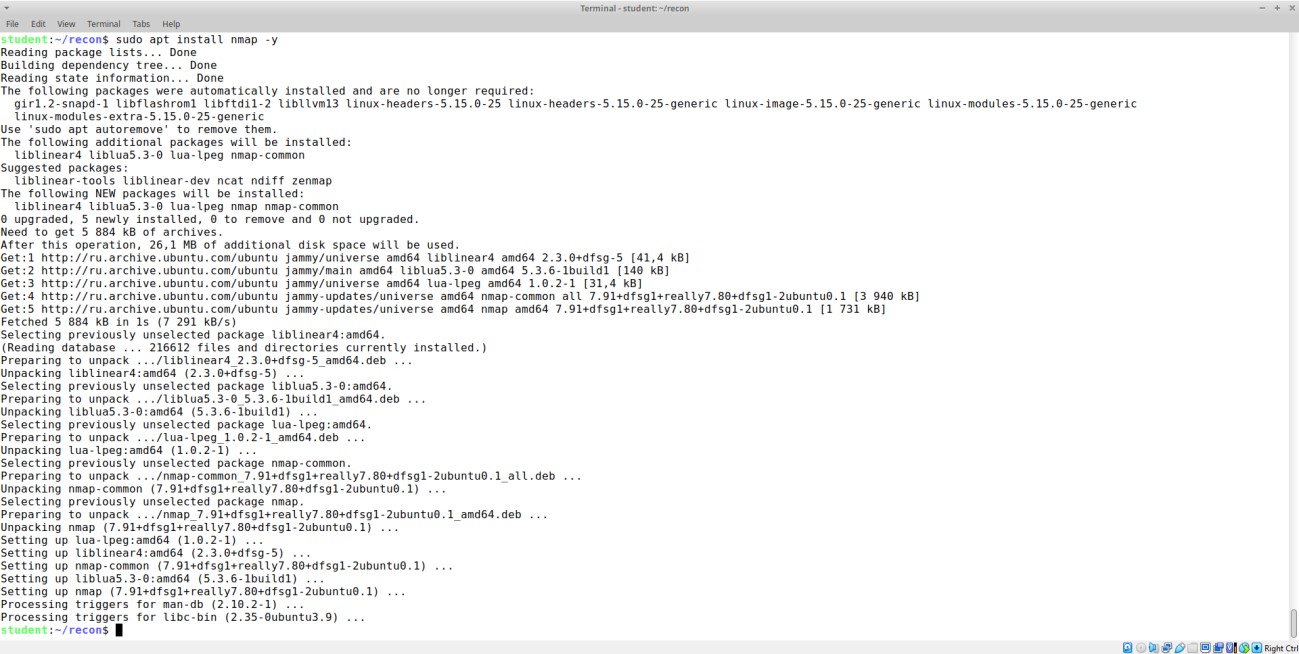
*Рис 22 Инициализация API-ключа и проверка его работы*

Регистрируемся на leakix.net, для получения api-ключ.



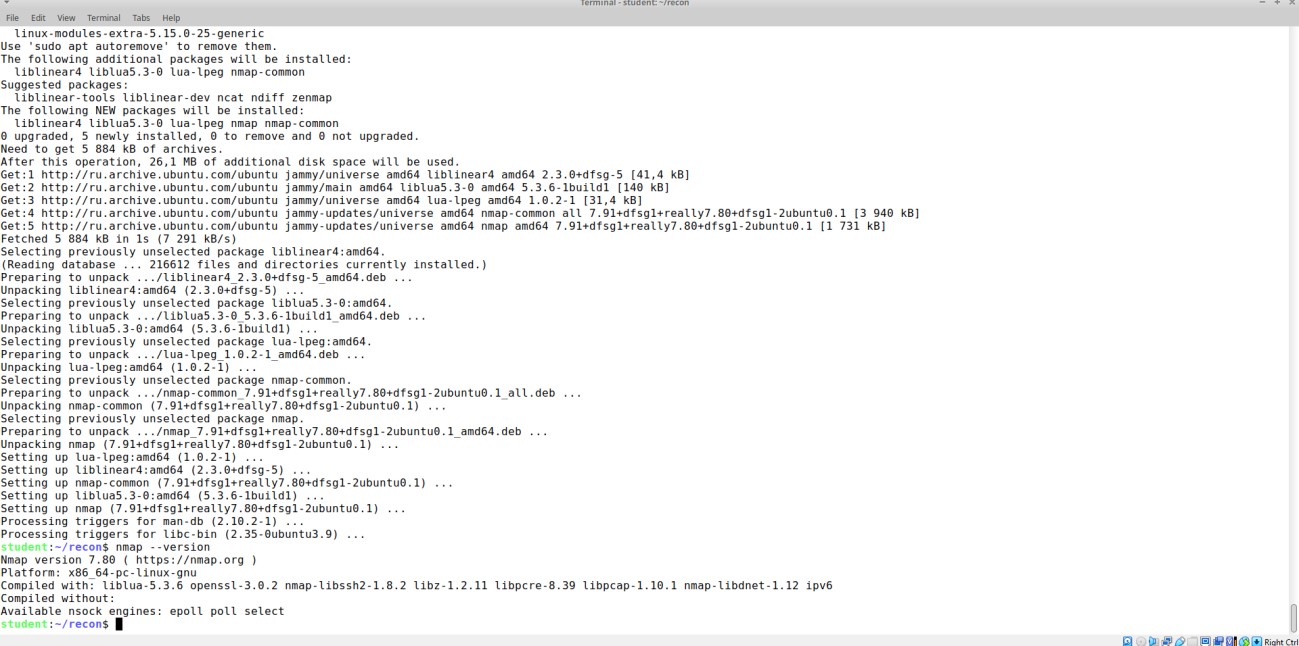
*Рис 23 Регистрация на сайте Leakix*

Устанавливаем nmap, утилиту для сканирование портов и сервисов, быстрое получение списка открытых портов и версий ПО.



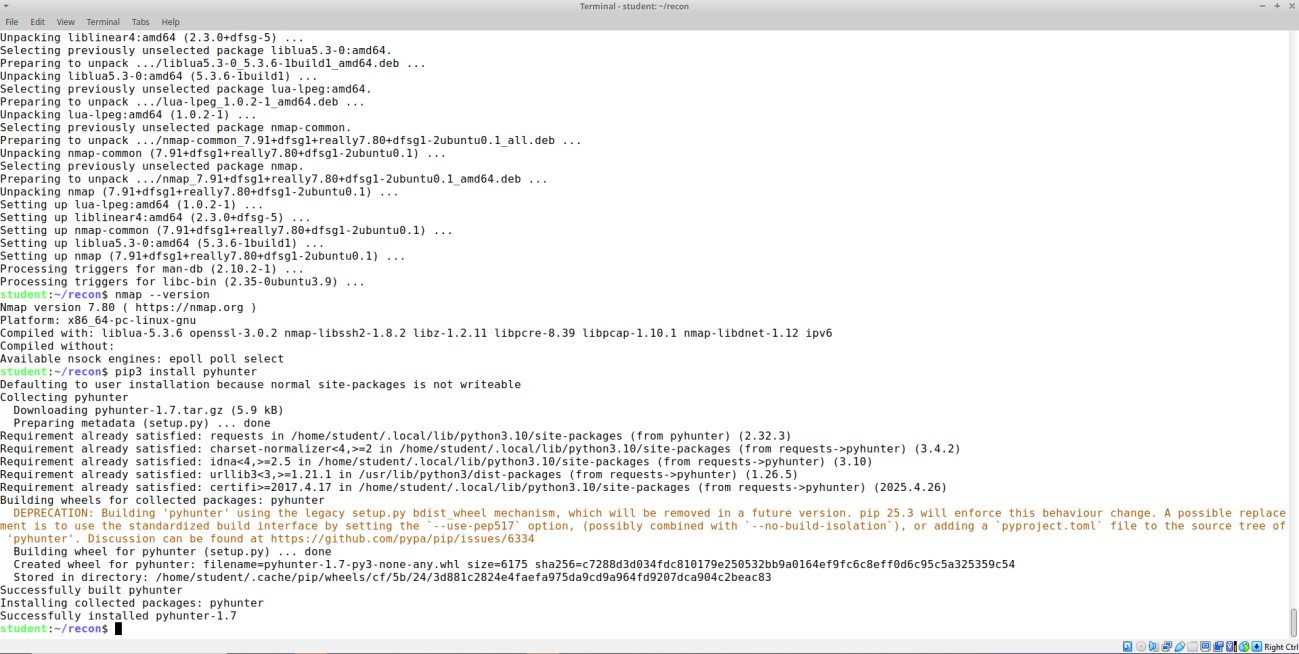
*Рис 24 Установка nmap*

Проверяем установку nmap.



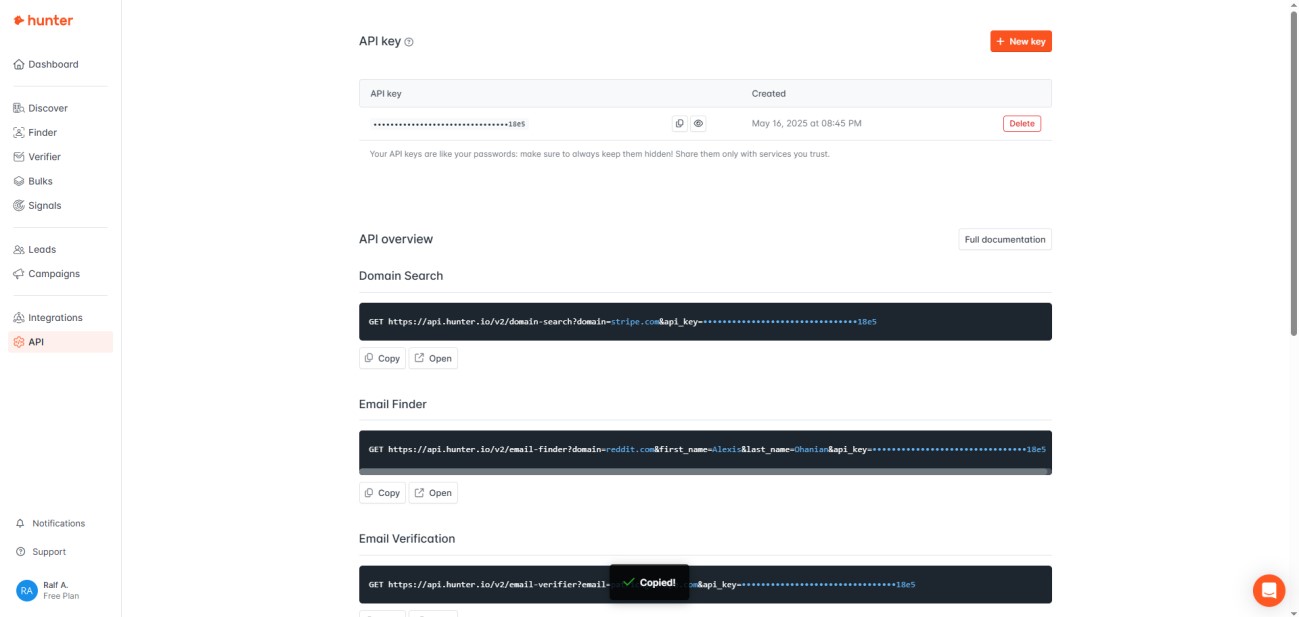
*Рис 25 Проверка nmap*

Устанавливаем pyhunter, для работы с hunter.io, с помощью команды “pip3 install pyhunter”.



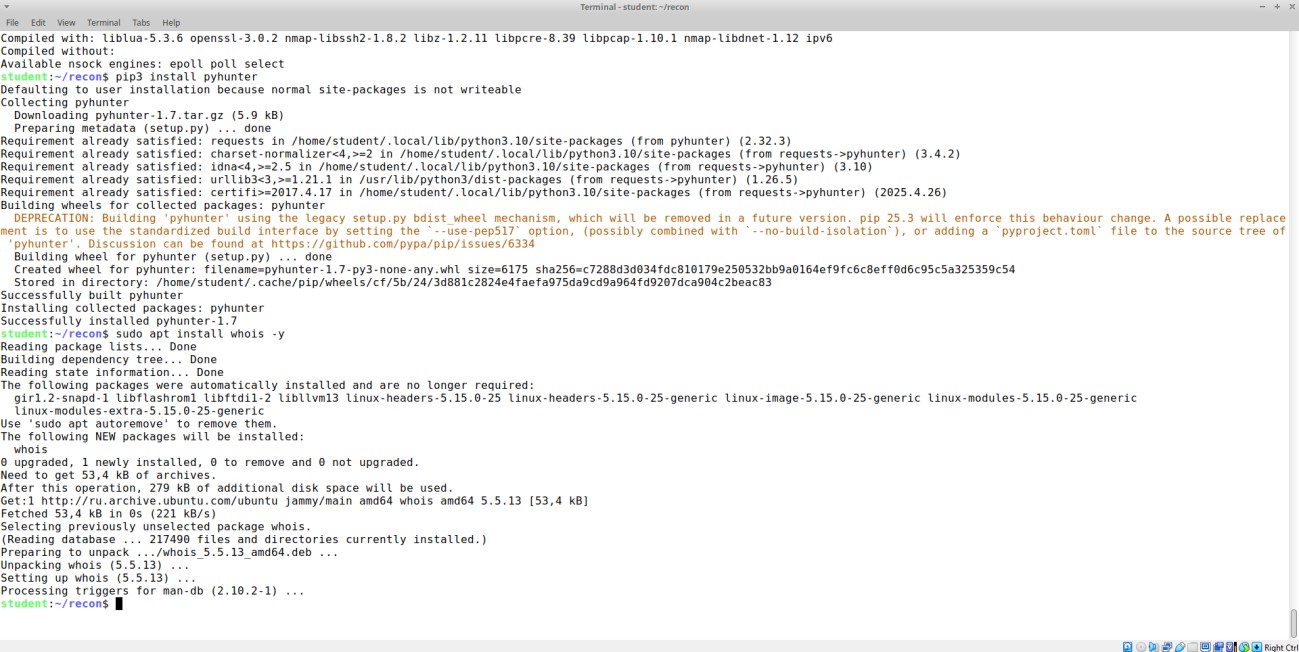
*Рис 26 Установка pyhunter*

Регистрируемся в hunter.io, для получения api-ключа.



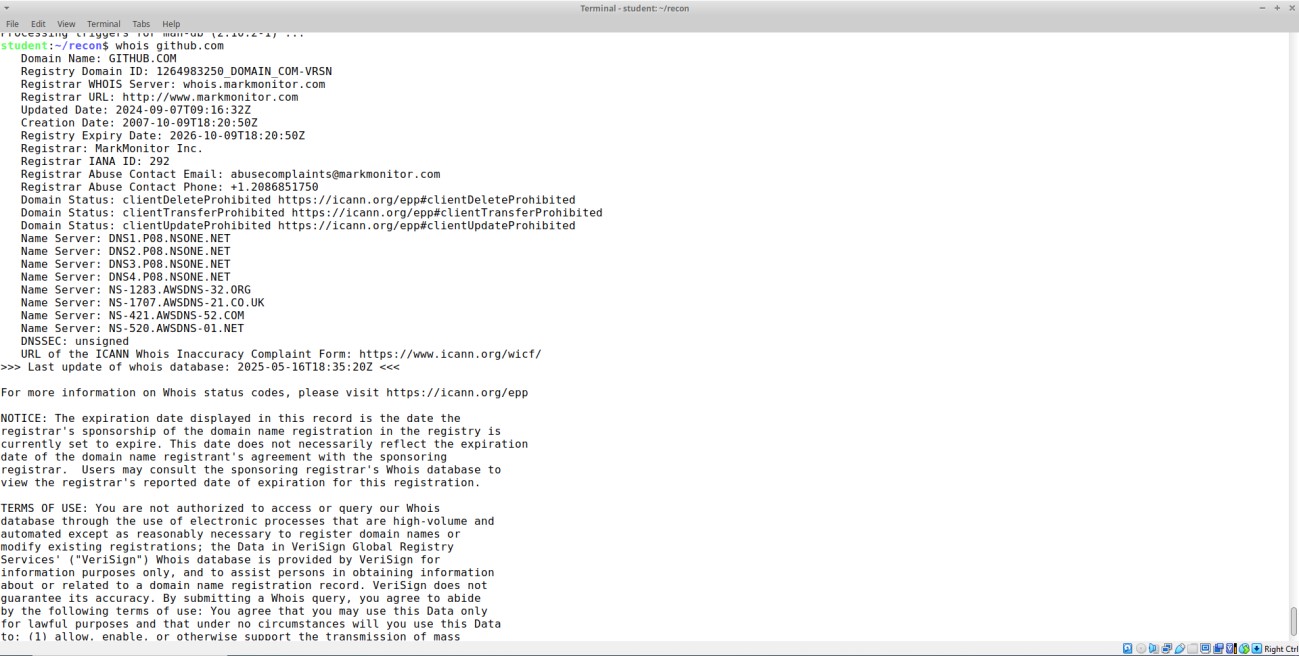
*Рис 27 Регистрация в hunter.io*

Установка whois, с помощью команды: “sudo apt install whois -y”



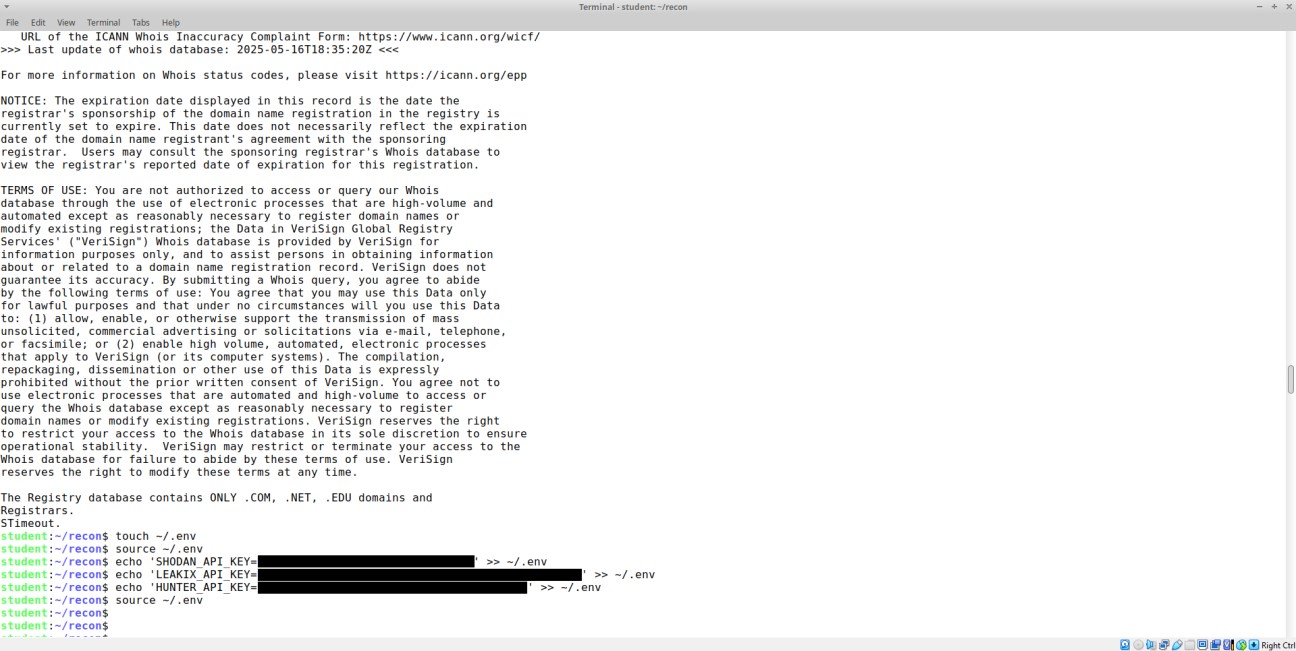
*Рис 28 Установка whois*

Проверка работы whois, запршиваем информацию о сайте github.com.



*Рис 29 Проверка whois*

Настройка API-ключей, для более удобного использования.



*Рис 30 Настройка API-ключей*

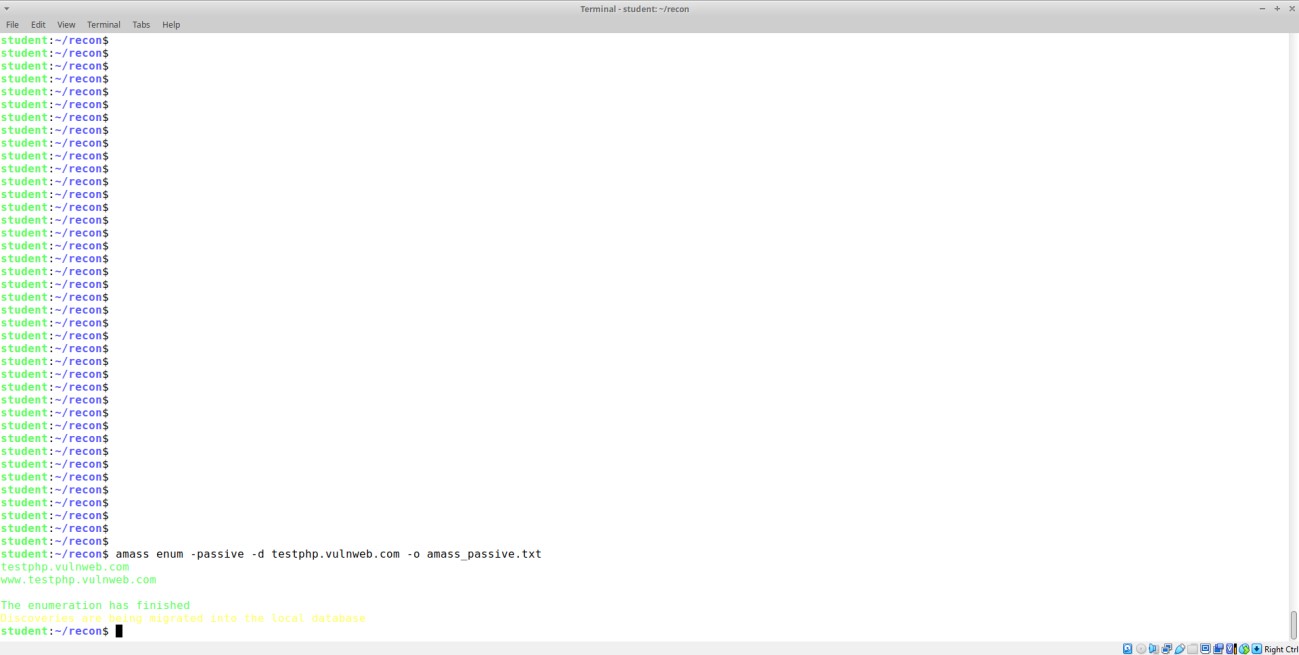
Пассивная разведка с Amass

*Вводим команду “amass enum -passive -d testphp.vulnweb.com -o amass\_passive.txt”* enum — режим сбора информации;

-passive — только пассивные источники (не будет прямого

взаимодействия с целью);

-d — домен цели;



*Рис 31 Результат проверки amass*

Активная разведка с Nmap

*Вводим команду “nmap -sS -Pn -p1-1000 testphp.vulnweb.com -oN nmap\_full.txt” .Было принято решение просканировать первые 1000 портов, которые являются самыми полярными, так как скан всех портов занимает очень много времени.*

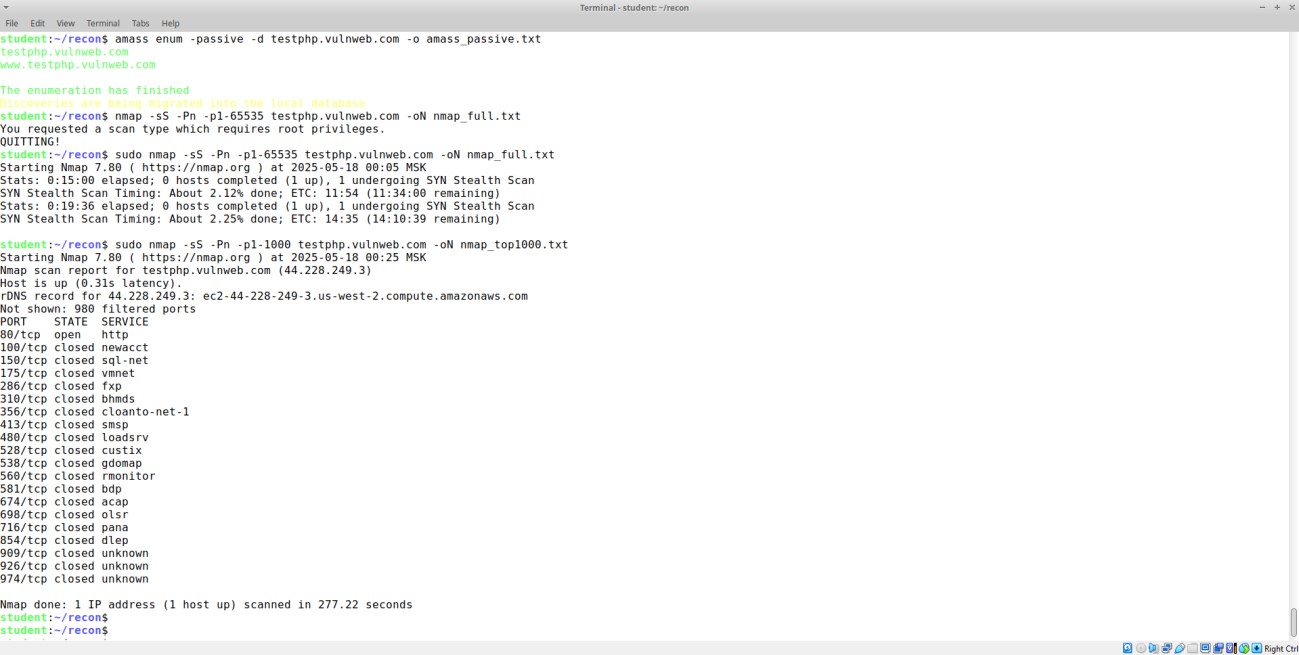
-sS — SYN-сканирование: полустелс, быстрый способ проверить открытые порты.

-Pn — пропустить ping, считать хост доступным.

-p1-1000 — все возможные порты.

-oN — сохранить в текстовом формате.

Открыт 80/tcp порт, 19 портов закрыты, другие порты фильтруются.

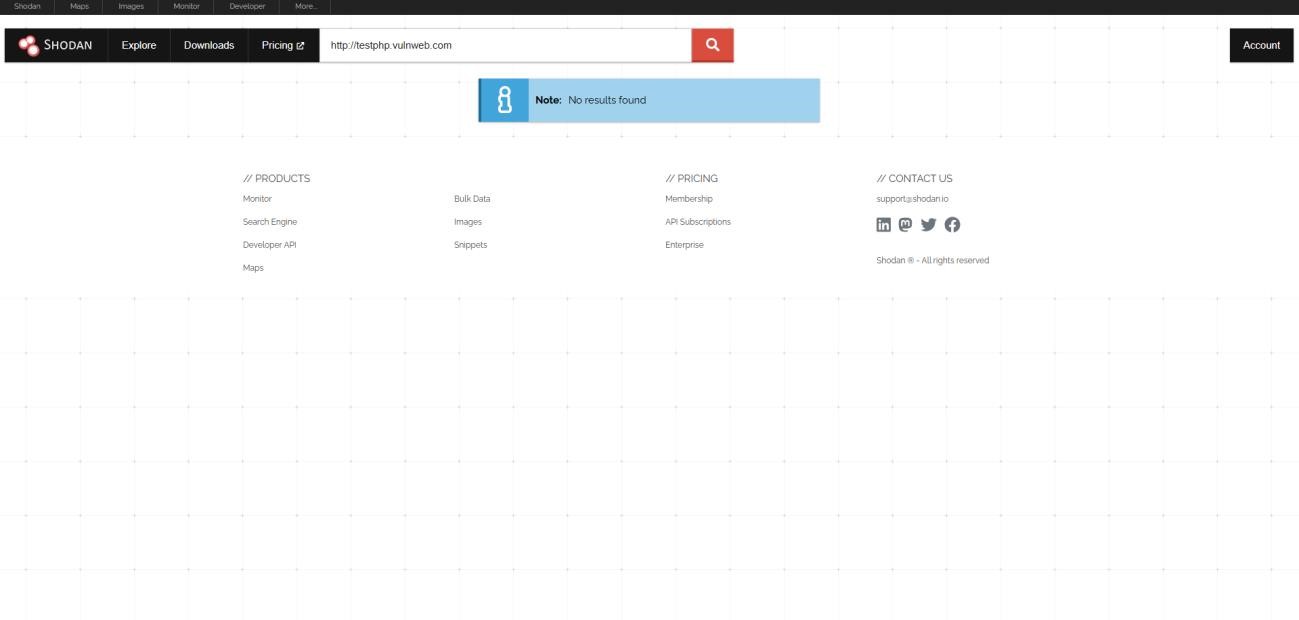


*Рис 32 Результат проверки nmap*

Для поиска в shodan, воспользуемся браузером, так как для использования через терминал, необходимо покупать кредиты, а для их получения требуется купить подписку на их сайте.

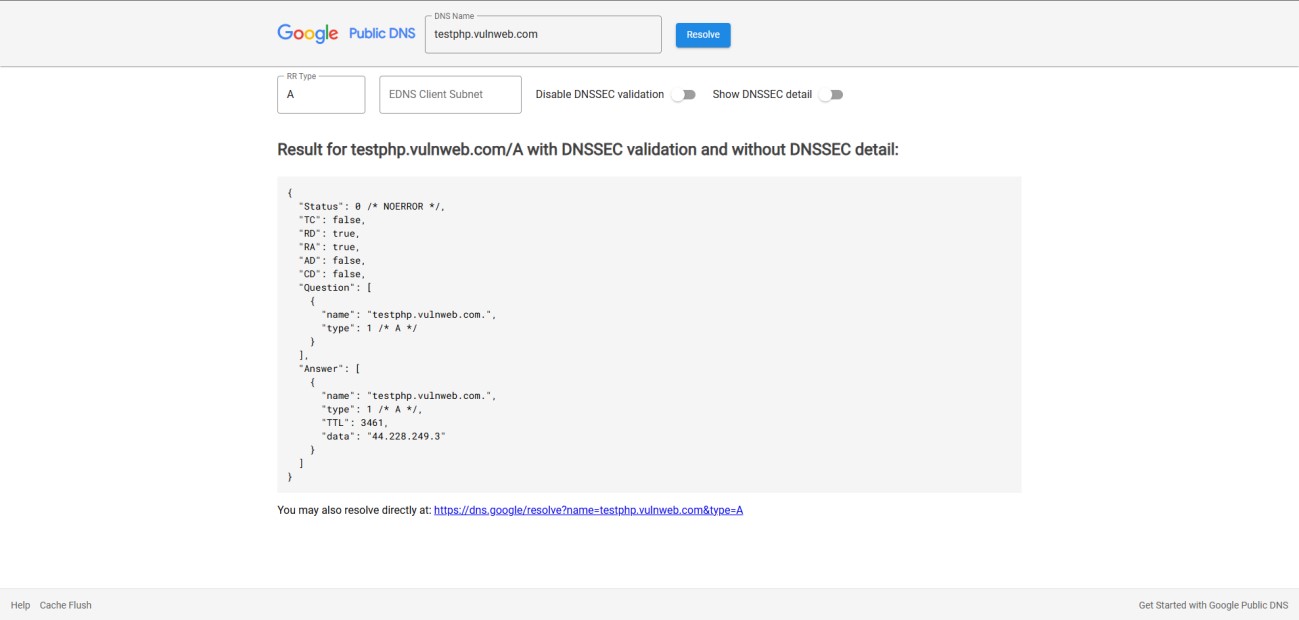


*Рис 33 Shoda требует кредиты*



*Рис 34 Поиск в браузере shodan по url страницы*

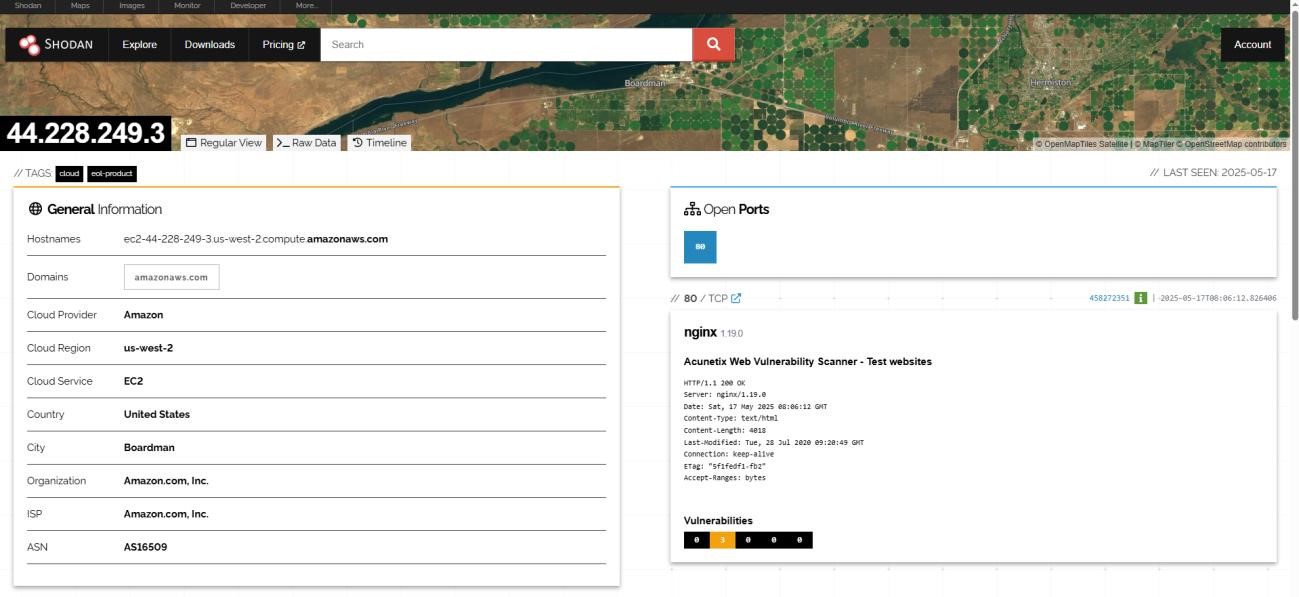
Узнаем IP-адрес страницы testphp.vulnweb.com, с помощью dns-сервера google.



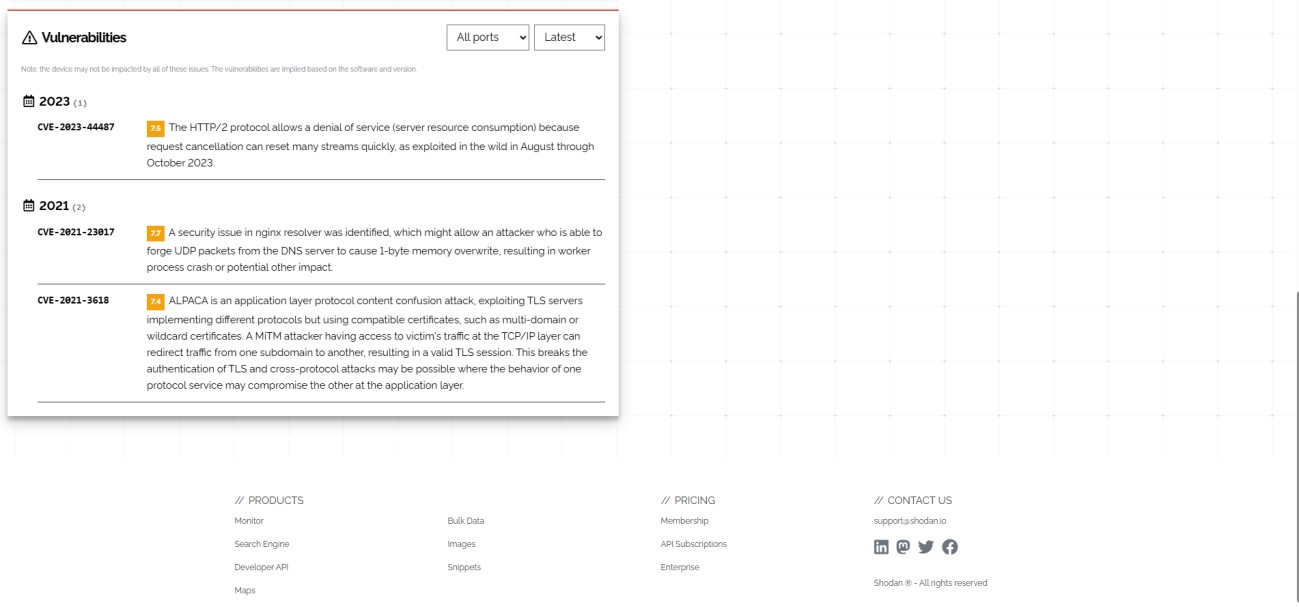
*Рис 35 IP-адрес testphp.vulnweb.com*

Проверяем IP-адрес а не сайт и получаем сводку информации:

( [https://www.shodan.io/host/44.228.249.3)](https://www.shodan.io/host/44.228.249.3)

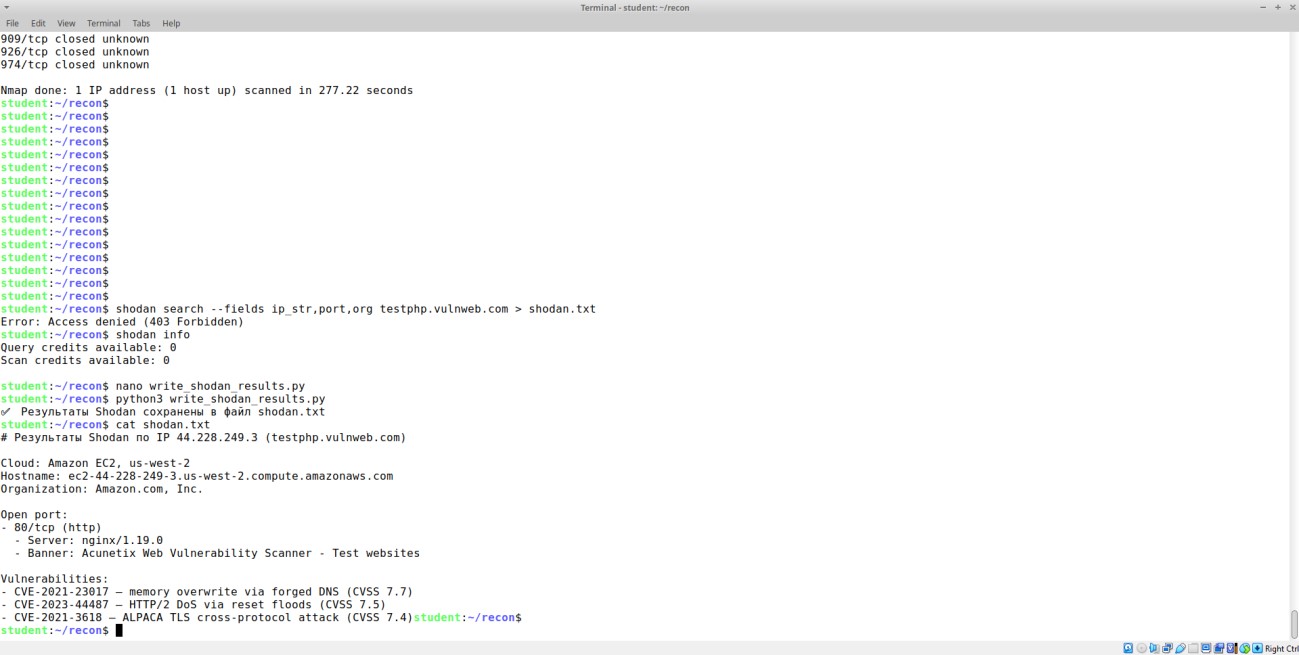


*Рис 36 1 часть результатов shodan*



*Рис 37 2 часть результатов shodan*

Записываем данные в txt файл.



*Рис 38 Запись данных в txt-файл*

Сводка данных из shodan

Таблица 4 Уязвимости (по версии nginx/1.19.0)

|  |  |  |
| --- | --- | --- |
| **CVE ID** | Уровень | **Описание** |
| **CVE-2021-23017** | 7.7 (High) | Уязвимость в DNS resolver nginx — возможен краш или overwrite |
| **CVE-2023-44487** | 7.5 (High) | DoS-атака через HTTP/2 — массовый сброс запросов |
| **CVE-2021-3618** | 7.4 (High) | ALPACA-атака — подмена TLS-трафика между субдоменами |

Общая информация

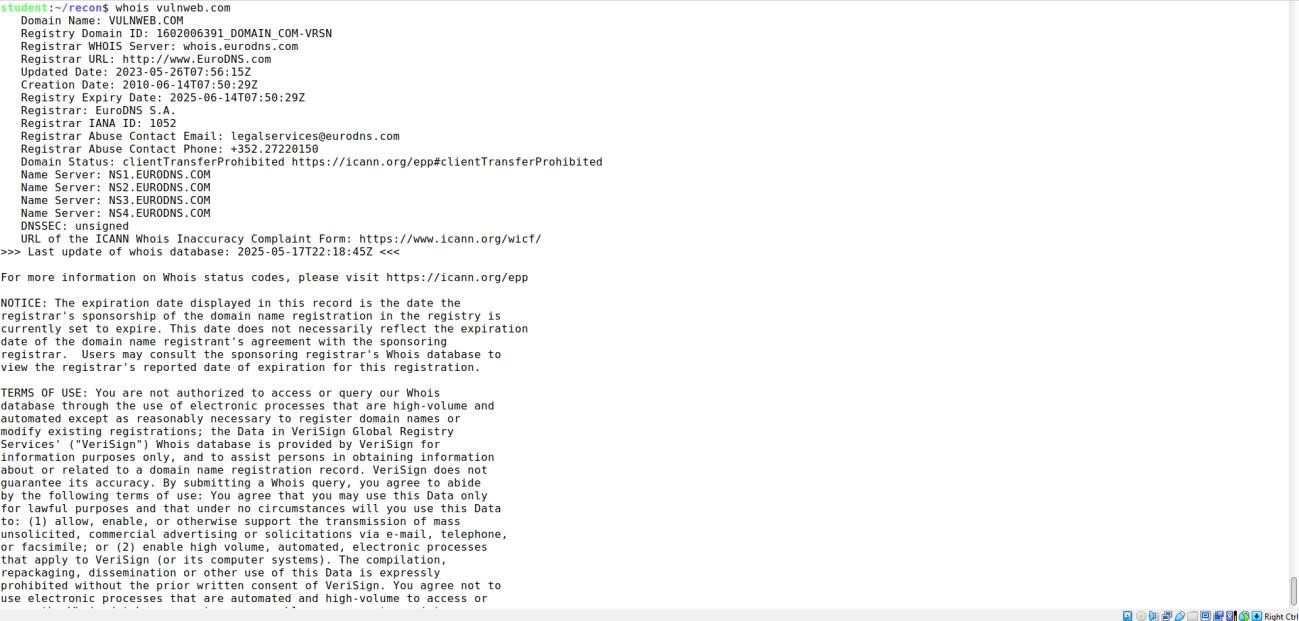
* IP-адрес: 44.228.249.3
* Обратное имя (rDNS): ec2-44-228-249-3.us-west-

2.compute.amazonaws.com

* Домен: amazonaws.com  Провайдер облака: Amazon EC2
* Регион: us-west-2 (Boardman, США)
* Организация / ISP: Amazon.com, Inc.
* ASN: AS16509

Открыт 80/tcp порт для http, с версией nginx/1.19.0

Просматриваем информацию о сайте vulnweb.com с помощью утилиты whois. И запишем в файл “whois.txt”, пользуясь командой “nano whois.txt”.



*Рис 39 Результаты whois*

Регистрационные данные

* Домен: vulnweb.com
* Дата создания: 2010-06-14
* Дата окончания: 2025-06-14
* Обновление данных: 2023-05-2

Регистратор (Registrar)

* Компания: EuroDNS S.A.
* IANA ID: 1052
* Сайт:
* Email для жалоб: legalservices@eurodns.com
* Телефон: +352.27220150 DNS-серверы
* NS1.EURODNS.COM
* NS2.EURODNS.COM
* NS3.EURODNS.COM
* NS4.EURODNS.COM

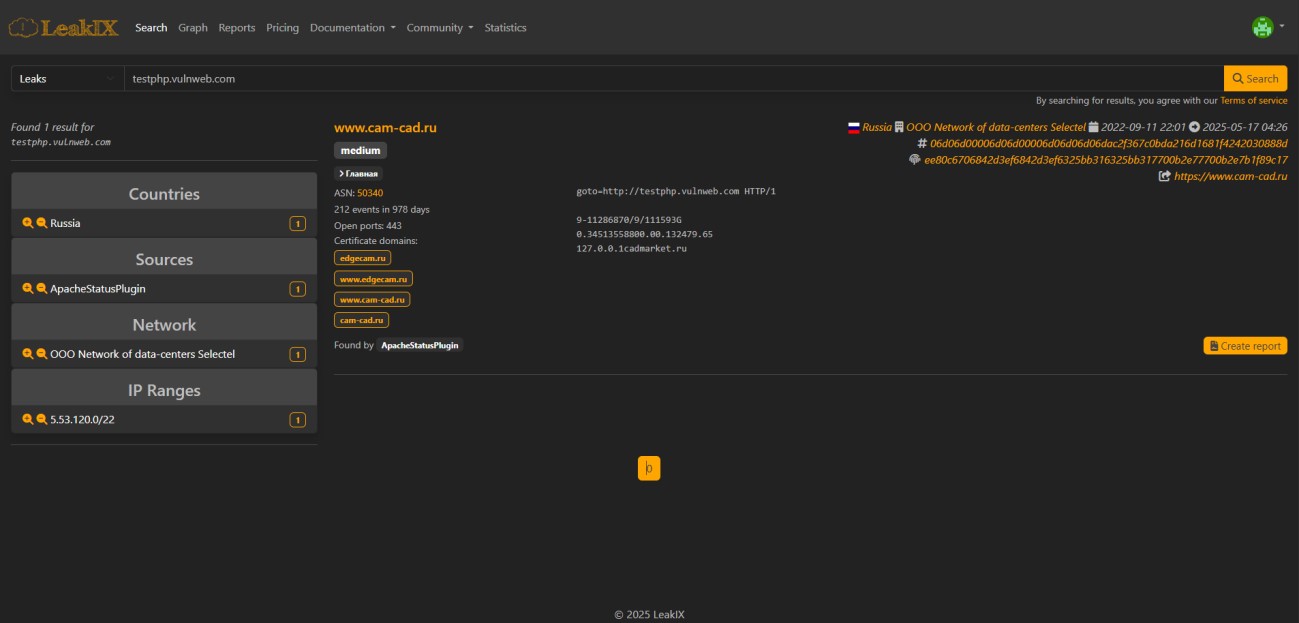
Статус домена : clientTransferProhibited. Это значит, что домен защищён от автоматического переноса к другому регистратору.

Производим поиск через сайт leakix.net, из-за невозможности напрямую импортировать данные(официального публичного JSON-API для прямого поиска нужного домена больше нет или он скрыт (и возвращает 404)).



*Рис 40 Leakix выдает ошибку при попытке получения через консоль*

[(https://leakix.net/search?scope=leak&q=testphp.vulnweb.com)](https://leakix.net/search?scope=leak&q=testphp.vulnweb.com%20)



*Рис 41 Результаты leakix*

Краткие выводы по LeakIX для testphp.vulnweb.com:

* Найдено 1 совпадение.
* Страна: Russia
* Источник: ApacheStatusPlugin
* Сеть: OOO Network of data-centers Selectel
* IP-диапазон: 5.53.120.0/22

Связанный хост:

* www.cam-cad.ru (ASN 50340, Amazon EC2)
* 212 событий за 978 дней
* Открыт порт 443, сервер nginx/1.19.0
* SSL-сертификат покрывает: edgecam.ru, www.edgecam.ru, www.cam-cad.ru, cam-cad.ru
* Есть редирект goto=http://testphp.vulnweb.com

Хеши первого события:

06d06d00006d06d00006d06d06d06dac2f367c0bda216d1681f4242030888d

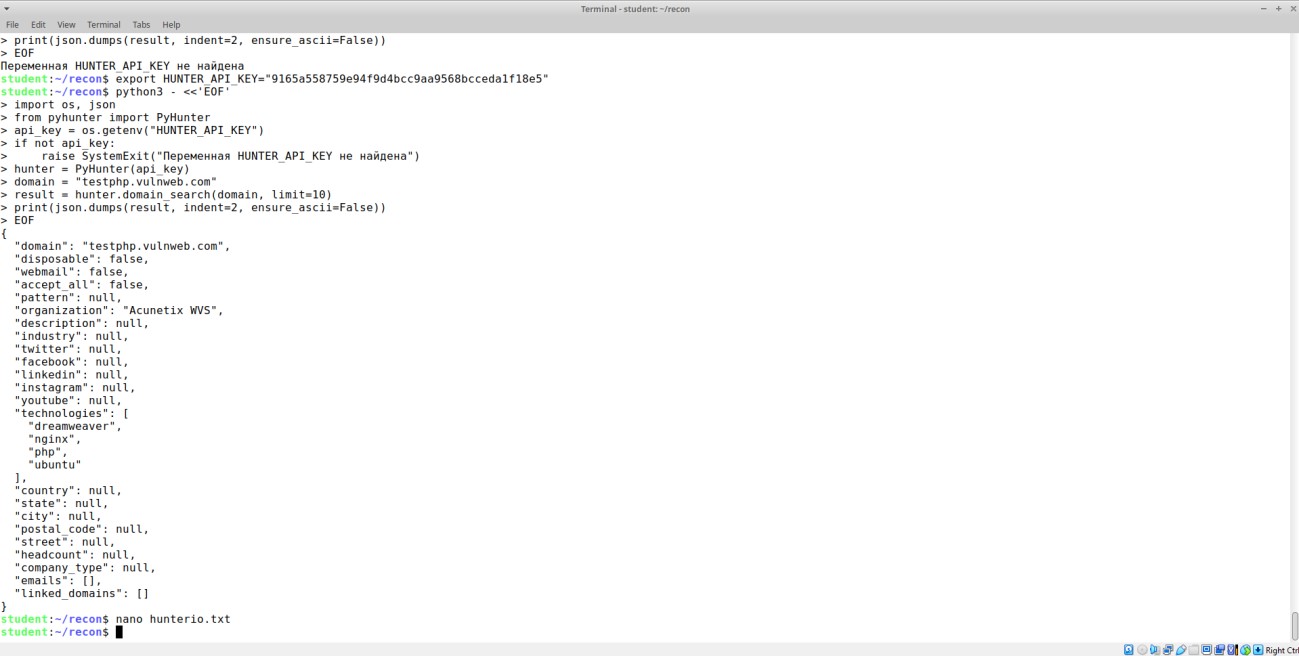
Запишем данные в txt-файл



*Рис 42 Запись данных leakix в txt-файл*

Вывод из Hunter.io, полученный через API и записываем результат в

“huntreio.txt”.



*Рис 43 Результат hunter.io и запись в файл*

domain: "testphp.vulnweb.com" — запрошенный домен. organization: "Acunetix WVS" — название организации, связанной с доменом (в данном случае, это демонстрационный сайт для сканера уязвимостей Acunetix).

technologies:

* "dreamweaver" — редактор/IDE от Adobe (возможно, в метаданных или сигнатурах HTML).
* "nginx" — веб-сервер.
* "php" — язык серверной логики.
* "ubuntu" — ОС сервера.

#### 4.3.3.3 Вывод по Вариативном заданию

Во время выполнения работы в процессе выполнения были освоены инструменты пассивной и активной разведки, такие как Nmap, Amass, Shodan и Hunter.io. Так же научился использовать API-сервисы, устанавливать и инициализировать ключи. Мне пришлось столкнулся с ограничениями API и отсутствием некоторых данных, что решалось через веб-интерфейсы (LeakIX,

Shodan). Так в процессе работы было освоено написание отчетов в формате Markdown.

Таблица 5 Финальный отчет

|  |  |
| --- | --- |
| **Источникк** | **Информация** |
| **Amass** | Найдено 2 поддомена: testphp.vulnweb.com, www.testphp.vulnweb.com |
| **Nmap** | Открыт порт: 80/tcp (http)Закрыты: 19 портов, остальные фильтруются |
| **Shodan** | IP: 44.228.249.3, Web-сервер: nginx/1.19.0Уязвимости: CVE-2021-23017, CVE-2023-44487, CVE-2021-3618 |
| **Hunter.io** | Организация: Acunetix WVSТехнологии: nginx, php, ubuntu, dreamweaver |
| **WHOIS** | Домен зарегистрирован в 2010, истекает в 2025. Регистратор: EuroDNS S.A. |
| **LeakIX** | Обнаружено совпадение с www.cam-cad.ru, SSL-сертификат перекрывает testphp.vulnweb.com. Найден редирект. |

С помощью фреймворков, как MITRE ATT&CK и Cyber Kill Chain, был произведен анализ найденных уязвимостей (CVE) из Shodan:

* CVE-2021-23017 (SYN Stealth scan, CVSS 7.7) — позволяет злоумышленнику вызвать краш процесса nginx, эксплуатируя DNS.
  + MITRE ATT&CK: техника T1203 — Exploitation for Client Execution.
  + Cyber Kill Chain: этап Exploitation.
* CVE-2023-44487 — HTTP/2 reset flood: вызывает DoS, перегружая ресурсы.
* MITRE ATT&CK: техника T1499 — Endpoint Denial of Service.
* Cyber Kill Chain: этап Delivery → Exploitation.
* CVE-2021-3618 — ALPACA-атака: кросс-протокольная подмена, возможен MitM.
  + MITRE ATT&CK: техника T1557 — Man-in-the-Middle.
  + Cyber Kill Chain: этап Command and Control.

Эти уязвимости могут быть использованы для:

* Нарушения доступности (DoS).
* Нарушения целостности трафика (TLS-подмена).
* Удалённого исполнения кода или сбора данных о системах.

**=**

Таблица 6 MITRE ATT&CK и Cyber Kill Chain

|  |  |  |  |
| --- | --- | --- | --- |
| **Компонент** | **Потенциальные угрозы** | **Этап Kill Chain** | **MITRE**  **ATT&CK** |
| WHOIS | DNS spoofing, социальная инженерия | Reconnaissance | T1583.001 |
| Hunter.io | Технологии, инфраструктура | Reconnaissance | T1592 |
| Amass | Поддомены, входные точки | Reconnaissance | T1590.002 |
| Nmap | Живые сервисы, fingerprinting | Reconnaissance  / Exploit | T1046 |
| Shodan | CVE, версионность  nginx | Exploitation | T1203,  T1499,  T1557 |

## 4.4 Личный вклад в проектную (учебную) практику и распределение времени

В ходе прохождения практики принимал активное участие в командной работе над проектом. Совместно с участниками группы изучал основы работы с системой контроля версий Git и научился оформлять репозиторий с использованием шаблонной структуры. Освоил синтаксис Markdown и участвовал в создании документации проекта.

На этапе разработки статического сайта подготовил все основные страницы, за исключением раздела «Журнал»(вкладку реализовал Бойков Т. А.), а также разработал и реализовал фирменное оформление сайта (единый стиль, графическое оформление карточек и блоков).

Совместно с командой решал технические проблемы, связанные с публикацией сайта на GitHub Pages, в частности — устранение ошибок в подключении пользовательских CSS-стилей.  
Дополнительно принял участие в посещении профильного мероприятия и в анализе одного из актуальных киберинцидентов.

Таблица 7 Личный вклад в выполненные задания

|  |  |  |
| --- | --- | --- |
| **Задание** | **Время (ч)** | **Сроки** |
| Git и Markdown | 3 | 20.03–22.03 |
| Сайт на Hugo +  Оформление | 20 | 27.03–19.05 |
| Мероприятие + отчет | 7 | 17.05 |
| Вариативное задание | - | - |
| Финальный отчет | 4 | 21.05 |
| Итого | 34 |  |

Таблица 8 Выполненные задания группой

|  |  |  |
| --- | --- | --- |
| **Задание** | **Время (ч)** | **Сроки** |
| Git и Markdown | 9 | 20.03–22.03 |
| Сайт на Hugo +  Оформление | 26 | 27.03–19.05 |
| Мероприятие + отчет | 7 | 17.05 |
| Вариативное задание | 28 | 05.05–19.05 |
| Финальный отчет | 4 | 21.05 |
| Итого | 72 |  |

# Заключение

В рамках проектной практики, проходившей во втором семестре 2025 года на базе Московского Политехнического университета по направлению «Информационная безопасность», был реализован комплекс заданий, охватывающих как технические, так и аналитические аспекты профессиональной деятельности.

Основной задачей практики стало формирование навыков работы с системами контроля версий (Git), оформление технической и организационной документации в формате Markdown, а также создание и развертывание статического веб-сайта с использованием генератора Hugo. В процессе работы был разработан и опубликован многостраничный информационный ресурс, отражающий содержание проекта GoSpot, структуру команды, хронологию разработки и взаимодействие с организацией-партнёром.

В дополнение к базовому заданию выполнена вариативная часть, включающая анализ методов внешней разведки корпоративной сети. Проведено детальное изучение и практическое применение инструментов OSINT и активной разведки, включая Amass, Nmap, Shodan, LeakIX, Hunter.io и другие. Также были рассмотрены и применены фреймворки MITRE ATT&CK и Cyber Kill Chain для классификации угроз и понимания этапов потенциальных атак.

Значимым этапом стало участие в Дне открытых дверей Московского Политеха, что позволило расширить представление об образовательной инфраструктуре и наладить связь с кураторами проектной деятельности. Материалы мероприятия были интегрированы в сайт, тем самым подчёркивая практико-ориентированную направленность дисциплины.

Все задачи, поставленные в рамках практики, включая публикацию сайта, оформление отчётов, взаимодействие с платформами GitHub, а также проведение прикладного анализа, были успешно реализованы. Командная работа, сопровождённая самостоятельным поиском решений и оформлением результатов в публичном виде, позволила участникам практики существенно углубить компетенции в области информационной безопасности и веб-разработки.

Практика продемонстрировала высокий уровень вовлечённости студентов в проектную деятельность и стала прочной основой для дальнейшего профессионального роста.

# Список использованных источников

1. Leakix // Leakix URL: <https://leakix.net/> (дата обращения: 17.05.2025).
2. Shodan Dashboard // Shodan URL: <https://www.shodan.io/dashboard> (дата обращения: 17.05.2025).
3. Hunter Dashboard // Hunter.io URL: <https://hunter.io/dashboard> (дата обращения: 17.05.2025).
4. Руководство Amass // Kali Tools URL: <https://kali.tools/?p=4325> (дата обращения: 17.05.2025).
5. Whois tool // Kali Linux URL: <https://www.kali.org/tools/whois/> (дата обращения: 17.05.2025).
6. Руководство nmap // Kali Tools URL: <https://kali.tools/?p=1317> (дата обращения: 16.05.2025).
7. MITRE ATT&CK Framework // MITRE URL: <https://attack.mitre.org/> (дата обращения: 17.05.2025).
8. Cyber Kill Chain // Darktrace URL: <https://www.darktrace.com/cyber-ai-glossary/cyber-kill-chain> (дата обращения: 17.05.2025).
9. Книга Pro Git // Git SCM URL: <https://git-scm.com/book/ru/v2> (дата обращения: 20.03.2025).
10. Основы CSS // MDN Web Docs URL: <https://developer.mozilla.org/ru/docs/Web/CSS> (дата обращения: 28.03.2025).
11. Creating the Content // MDN Web Docs URL: <https://developer.mozilla.org/ru/docs/Learn_web_development/Getting_started/Your_first_website/Creating_the_content> (дата обращения: 28.03.2025).
12. Getting Started with Hugo // Hugo URL: <https://gohugo.io/getting-started/usage/> (дата обращения: 29.03.2025).
13. Microsoft. Microsoft actions following attack by nation-state actor Midnight Blizzard [Электронный ресурс]. – URL: <https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard> (дата обращения: 08.04.2025).
14. Microsoft. Midnight Blizzard: Guidance for nation-state attack [Электронный ресурс]. – URL: <https://www.microsoft.com/en-us/security/blog/2024/01/19/midnight-blizzard-guidance-for-nation-state-attack> (дата обращения: 08.04.2025).