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

**ЛАБОРАТОРНАЯ РАБОТА № 4**

1. **«Проведение пассивной разведки заданного хоста»**
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

Провести пассивную и активную разведки заданного хоста и определить степень его защищенности.

# ход решения

## Пассивная разведка

Сначала с помощью whois была получена информация о датах создания и последнем изменении на сайте, контактная информация и т.д.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 1 – Общая информация о сайте

Изображение выглядит как текст, снимок экрана, меню, Шрифт

Автоматически созданное описание

Рисунок 2 – Контактная информация

С помощью сайта 2ip.ru было проверено, что с данного ip не было спам рассылок, а также данный сайт относится к безопасным.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 3 – Информация о безопасности сайта

Также получена информация о сроках ssl.

Изображение выглядит как текст, снимок экрана, Шрифт, алгебра

Автоматически созданное описание

Рисунок 4 – Период действия SSL

## Активное сканирование веб-сервера

С помощью securityheaders.com был получен и проанализирован заголовок GET-запроса. Так было выяснено, что установлено серверное ПО Apache и платформа приложений php/8.1.28.

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Рисунок 5 – Http-заголовки безопасности

Настроены следующие http-заголовки для обеспечения безопасности:

* X-Content-Type-Options — это HTTP-заголовок, который защищает веб-приложения от атак на определение типа MIME. Когда значение заголовка X-Content-Type-Options установлено на «nosniff», браузер всегда использует тип MIME, объявленный в заголовке Content-Type вместо того, чтобы пытаться определить тип MIME на основе содержимого файла.
* X-Frame-Options — это заголовок HTTP-ответа от сервера, который служит инструкцией для браузера и разрешает или запрещает отображение страниц сайта во фрейме. Когда значение заголовка установлено на «SAMEORIGIN», браузер разрешает загрузку страниц сайта во фрейме, только если фрейм и страница расположены на одном домене.

Также была получена информация о следующих уязвимых местах.

Изображение выглядит как текст, Шрифт, число, веб-страница

Автоматически созданное описание

Рисунок 6 – Отсутствующие http-заголовки

Далее утилитой nmap были определены ОС, открытые порты и запущенные на них службы, а также возможные уязвимости.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 7 – Информация об открытых портах и ОС

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 8 – Информация о запущенных службах

Была обнаружена уязвимость SSL POODLE.

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок 9 – Вывод уязвимостей, найденных через nmap

Через сайт pentest-tools.com были выявлены следующе угрозы.

Изображение выглядит как текст, линия, число, Шрифт

Автоматически созданное описание

Рисунок 10 – Уровень опасности найденных уязвимостей

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 11 – Уязвимость из-за использования php/8.1.28

Изображение выглядит как текст, снимок экрана, число, документ

Автоматически созданное описание

Рисунок 12 – Уязвимости с низким уровнем опасности

# Выводы

По результатам проведенного исследования хоста с помощью пассивного сканирования из открытых источников были получены сведения о хосте и домене (регистрация, контактные данные ответственных лиц, местоположение). При исследовании ответов сервера был выявлен ряд слабостей, например, раскрытие чувствительной информации, такой как название сервера и версия ПО. Данная информация может быть полезна злоумышленнику при подготовке атаки (можно, например, использовать существующие уязвимости). При проведении активного сканирования хоста были выяснены открытые порты, версия ОС сервера и наличие уязвимого протокола SSLv3.

Таким образом, защищенность сайта удовлетворительная. Разработчикам рекомендуется обновить версии используемого ПО, убрать чувствительную информацию и добавить http-заголовки обеспечивающие дополнительную безопасность.