

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

**«Дальневосточный федеральный университет»**

(ДВФУ)

|  |
| --- |
|  |
| **ИНСТИТУТ МАТЕМАТИКИ И**  **КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)** |

**Департамент морских арктических технологий**

**ОТЧЁТ**

**по практике**

УЧЕБНАЯ ПРАКТИКА. НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА (ПОЛУЧЕНИЕ ПЕРВИЧНЫХ НАВЫКОВ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ)

|  |  |  |
| --- | --- | --- |
|  |  | Выполнил студент  гр. М9121-09.04.01кб  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. С. Пугачев |
| Отчет защищен:  с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ( подпись) (И.О. Фамилия)  «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г. |  | Проверил старший преподаватель  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** С. С. Зотов |
| Регистрационный № \_\_\_\_\_\_  «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г.  \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ( подпись) (И.О. Фамилия) |  | Практика пройдена рассредоточено  в срок  с « 27 » сентября 2021 г.  по « 22 » января 2022 г.  в Дальневосточном Федеральном Университете |

г. Владивосток

2022

**Оглавление**

[Введение 3](#_Toc94126709)

[1. Индивидуальный план научно-исследовательской работы. 5](#_Toc94126710)

[2. Обоснование актуальности выбранной темы 5](#_Toc94126711)

[3. Решение прикладной задачи в выбранном направлении 6](#_Toc94126712)

[Заключение 11](#_Toc94126713)

[Список литературы 12](#_Toc94126714)

## Введение

Вид практики – учебная.

Тип практики – научно-исследовательская работа (практика).

Способ проведения - стационарная (возможен выездной способ).

Форма проведения практики – рассредоточенная (1, 2, 3, 4 семестры).

Местом проведения практики являются структурные подразделения ДВФУ или сторонние организации в соответствии с заключенными с ДВФУ договорами, обладающие необходимым кадровым и научно-техническим потенциалом.

Сроки проведения Учебной практики (Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)) регламентируются графиком учебного плана по направлению 09.04.01 Информатика и вычислительная техника, программа «Кибербезопасность».

Целями учебной практики являются:

* закрепление теоретических знаний, полученных во время аудиторных занятий и учебных практик;
* приобретение профессиональных навыков и умений;
* собор необходимых материалов для научно-исследовательской работы и написания выпускной квалификационной работы магистра.

Задачи учебной практики:

* сбор патентных и литературных источников по разрабатываемой теме с целью их использования при выполнении выпускной квалификационной работы;
* изучение методов исследования и проведения экспериментальных работ;
* применение методов анализа и обработки экспериментальных данных;
* построение физических и математических моделей процессов и явлений, относящихся к исследуемому объекту;
* освоение информационных технологий в научных исследованиях, программные продукты, относящиеся к профессиональной сфере;
* совершенствование аналитической деятельности при решении практических задач;
* формирование практические умения и навыки в профессиональной деятельности;
* сбор необходимых исходных данных и рабочих материалов для выполнения научно-исследовательских работ магистрантов при выполнении выпускной квалификационной работы.

## Индивидуальный план научно-исследовательской работы.

***Подготовка научно–исследовательской части ВКР***

1. Составление плана научно-исследовательской работы (НИР);
2. Обоснование актуальности темы, постановка цели и определение задач НИР;
3. Решение прикладной задачи в выбранном направлении;
4. Подготовка и защита отчета о практике.

## 2. Обоснование актуальности выбранной темы

В современном мире информационные технологии развиваются с каждым днём всё быстрее. Однако одновременно с появлением систем информационной безопасности и понятия «периметр» стал проводиться анализ защищённости компаний и отдельных компонентов их инфраструктуры. Одним из инструментов такого анализа является тест на проникновение, или пентест.

Целью тестирования является обнаружение возможных уязвимостей и недостатков, способных привести к нарушению конфиденциальности, целостности и доступности информации, спровоцировать некорректную работу системы или привести к отказу от обслуживания, а также спрогнозировать возможные финансовые потери и экономические риски. Тестирование затрагивает как виртуальный уровень, так и физический.

По результатам тестирования на проникновение дается оценка возможностей текущего уровня защищённости выдержать попытку вторжения потенциального злоумышленника, данные о количестве времени и ресурсов, требуемых для успешной атаки на заказчика. В случае выявления уязвимостей в обязательном порядке составляется список [рекомендаций по устранению](https://rtmtech.ru/services/pentest/) вышеуказанных уязвимостей.

Суть работ заключается в моделировании действий злоумышленника, намеренного получить доступ к информационным системам заказчика и нарушить целостность, конфиденциальность либо доступность принадлежащей заказчику информации. Самыми частыми объектами исследований являются:

* системы управления базами данных;
* сетевое оборудование;
* сетевые службы и сервисы (например, электронная почта);
* средства защиты информации;
* прикладное программное обеспечение;
* серверные и пользовательские операционные системы.

## 3. Решение прикладной задачи в выбранном направлении

Для решение прикладной задачи по пентесту была выбрана машина «Horizontall» (рисунок 1).

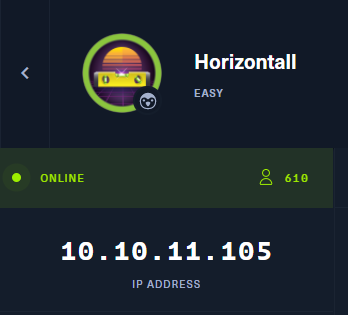


Рисунок 1 - Название машины

Как показано на рисунке 2, данная машина имеет CVE уязвимость.

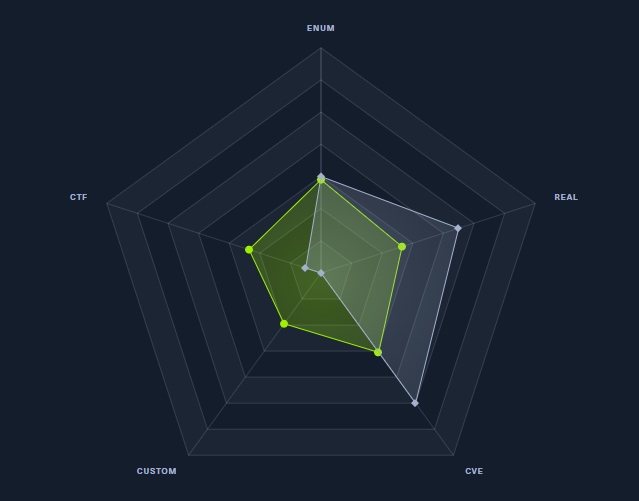


Рисунок 2 - Уязимость машины

Сначала необходимо проверить подключение VPN и просмотреть присвоенный IP адрес (рисунок 3).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3 - IP-адрес атакующей машины

Затем следует просканировать открытые порты атакуемой машины (рисунок 4).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 4 - Сканирование портов

Сканирование показало, что порт 80 открыт. Добавим *horizontal.htb* в локальный DNS и перейдем на данную страницу (рисунок 5).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 5 - Главная страница

Данная страница не содержит какой-либо нужной информации. Тогда, используя встроенную утилиту *DirBuster* в *Kali Linux*, стоит просканировать на наличие скрытых страниц (рисунок 6).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 6 - Сканирование скрытых страниц

По завершению сканирования нашелся файл *app.c88eb462.js*. Открыв данную страницу, можно найти ссылку на подкаталог *http://api-prod.horizontall.htb/reviews* (рисунок 7).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 7 - Страница app.c88eb462.js

Страница *http://api-prod.horizontall.htb/reviews* также не содержит никакой полезной информацией. Поэтому неоюходимо просканировать страницу *http://api-prod.horizontall.htb/* на подкаталоги. В результате сканирования нашелся подкаталог /admin/ (рисунок 8).

Изображение выглядит как стол

Автоматически созданное описание

Рисунок 8 - Результат сканирования страницы

Перейдя на данную страницу, получим панель для входа администратора (рисунок 9).

Изображение выглядит как текст, снимок экрана, монитор

Автоматически созданное описание

Рисунок 9 - CMS форма Strapi

Для данной CMS есть общедоступный эксплойт Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated) (рисунок 10).

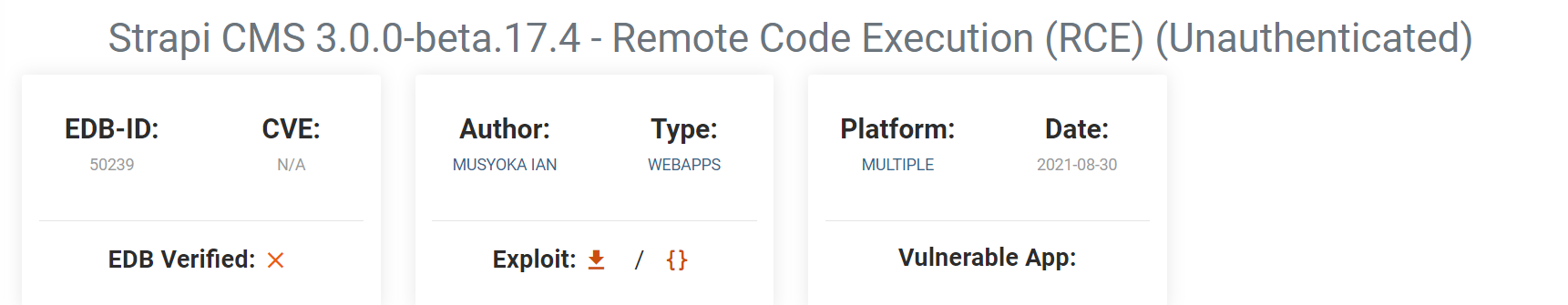


Рисунок 10 - Эксплойт

Необходимо запустить данный эксплойт (рисунок 11) и параллельно начать прослушивание на порту 6199 (рисунок 12).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 11 - Запуск эксплойта

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 12 - Прослушивание порта

Теперь имея удаленный доступ в качестве пользователя strapi можно найти флаг в файле user.txt (рисунок 13).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 13 - Нахождение флага

В результате работы в директории /home/developer был найден файл user.txt, содержащий в себе флаг.

## Заключение

В результате учебной практики были собраны все необходимые исходные данные для проведения научно-исследовательской работы в рамках ВКР, а именно:

* Составлен план научно-исследовательской работы (НИР);
* Произведено обоснование актуальности темы НИР;
* Решена прикладная задача выбранного направления.

## Список литературы

1. А.С. Кленин. Методические указания по подготовке проектных работ: для студентов направления «Прикладная математика и информатика (профиль системное программирование)» и «Прикладная информатика». Владивосток: Дальневост. федерал. ун-т, 2016. -72с.
2. ГОСТ 7.32-2001 Отчет о научно-исследовательской работе. Структура и правила оформления. Москва, 2001 - 19c.
3. Кузнецов И.Н. Основы научных исследований: учебное пособие. М.: Дашков и К, 2012.
4. Сабитова Р.Г. Основы научных исследований. Владивосток: ДГУ, 2005.