

Российский университет транспорта (МИИТ)

Институт транспортной техники и систем управления

Кафедра «Управление и защита информации»

Отчет по практике

«Производственная практика: технологическая практика»

Выполнил: Дроздов А.Д., студент
группы ТКИ-342

Руководитель практики от
организации: Шилкин И.Е,
программист

Руководитель практики от учебного
заведения: Логинова Л.Н., доцент
кафедры УиЗи, к.т.н.

Москва 2023

СОДЕРЖАНИЕ

ПЛАН ПРОХОЖДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ.....	3
ВВЕДЕНИЕ	4
ТЕОРЕТИЧЕСКАЯ ЧАСТЬ	5
1.1. Основы информационной безопасности.....	5
1.2. Вопросы ИБ в РФ	5
ПРАКТИЧЕСКАЯ ЧАСТЬ	7
2.1. Разработка документов в отношении обработки ПД	7
2.2. Работа с Linux	8
ЗАКЛЮЧЕНИЕ	13
СПИСОК ЛИТЕРАТУРЫ.....	14

ПЛАН ПРОХОЖДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Календарный (понедельный) график прохождения производственной практики отображен в таблице 1.

Таблица 1 – Понедельный план практики

№ п/п	Краткое описание	Дата
1	Вводный инструктаж в организации, техника безопасности	29.06.23
2	Описание организации и комплексный анализ состояния информационной безопасности организации	30.06.23 – 06.07.23
3	Изучение нормативной базы ИБ, рассмотрение основ по работе с Linux	07.07.23 – 14.07.23
4	Применение полученной информации на практике	15.07.23 – 18.07.23
5	Подведение итогов и исправление недочётов	19.07.23 – 20.07.23
6	Получение документов о прохождении практики, подготовка отчета	21.07.23

ВВЕДЕНИЕ

Осуществление производственной практики имеет важное значение в процессе получения высшего образования и способствует развитию профессиональных навыков и компетенций студентов в сфере информационной безопасности. Она предоставляет студентам возможность применять полученные знания и умения на практике, а также приобретать необходимый опыт работы в данной области. Практика дает возможность ознакомиться с основными видами деятельности в области информационной безопасности и развить профессиональные навыки, которые являются неотъемлемыми для успешной карьеры в этой сфере.

Целью производственной практики является приобретение практических навыков и опыта в области обеспечения информационной безопасности, а также применение теоретических знаний на практике.

Задачами производственной практики являются:

1. Получение опыта самостоятельной профессиональной деятельности.
2. Получение практических навыков в области анализа и оценки рисков информационной безопасности.
3. Изучение законодательных и нормативных требований в области информационной безопасности и их применение на практике.
4. Повышение осведомленности пользователей в вопросах информационной безопасности и проведение различных тренировок.
5. Определение и оценка уязвимостей компьютерных систем и сетей.

Производственная практика была пройдена в Государственном бюджетном учреждении здравоохранения города Москвы "Детская городская поликлиника №86 Департамента здравоохранения города Москвы" (ГБУЗ "ДГП №86 ДЗМ").

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1. Основы информационной безопасности

С увеличением различных информационных технологий во всех сферах деятельности увеличивается число угроз и кибератак, а значит возникает необходимость в информационной безопасности, обеспечивающая конфиденциальности, целостности, доступности информации и защиту от несанкционированных действий.

В России актуальность вопросов информационной безопасности особенно высока. Национальный информационный ресурс "Интернет" в нашей стране является объектом повышенного внимания, как со стороны государственных структур, так и со стороны киберпреступников. Защита государственных информационных ресурсов, инфраструктуры коммуникаций и критически важных объектов является одним из приоритетов государственной политики Российской Федерации.

1.2. Вопросы ИБ в РФ

Изучая вопросы информационной безопасности, можно выделить основные группы:

1. Защита информационных систем и данных, включающая в себя работу с антивирусами, системами обнаружения вторжений, шифрованием и другими технологиями.
2. Защита персональных данных.
3. Киберпреступления – важное направление ИБ по борьбе с кибератаками, хакерами, вредоносными программами, фишингом и интернет-мошенничеством.
4. Кибербезопасность государственных систем – обеспечение защиты государственных информационных ресурсов и персональных данных граждан является приоритетом для России. В этой области уделяется особое внимание разработке и внедрению мер по защите

информационных систем государственных учреждений и критически важных объектов.

Далее, к указанным направлениям информационной безопасности рассмотрим нормативную базу – таблица 2.

Таблица 2 – Нормативная база ИБ

Направление	Наименование документа
Защита персональных данных	УП №188, ПП №1119, ФЗ №152, 21 Приказ ФСТЭК, 55 Приказ ФСТЭК
Защита информационных систем и данных	ФЗ №98, УП №188, СТР-К, 17 Приказ ФСТЭК
Кибербезопасность государственных систем	ПП №676, 17 Приказ ФСТЭК

ПРАКТИЧЕСКАЯ ЧАСТЬ

Руководителем практики был установлен перечень должностных обязанностей практиканта. Проведен инструктаж по технике безопасности.

Процесс выполнения производственной практики состоял из двух частей. Первая – работа с нормативной базой для составления политики оператора (ГБУЗ "ДГП №86 ДЗМ") по обработке персональных данных (далее - ПД).

Следующий немаловажный этап на практике – это техническая часть практики, работа с операционной системой Linux.

2.1. Разработка документов в отношении обработки ПД

В соответствии с федеральным законом №152 "О персональных данных", статья 18.1. пункт 1 был создан документ, включающий в себя:

1. Цели обработки ПД.
2. Категории и полный перечень обрабатываемых ПД.
3. Способы и сроки обработки ПД.
4. Сроки хранения ПД.

Для полноценного рассмотрения данного вопроса были использованы документы, регулирующие трудовое законодательство РФ, где указывается необходимый перечень персональных данных сотрудников организации. А также документы, регулирующие сроки хранения медицинской документации, для такого субъекта персональных данных, как пациент.

Далее, на основании политики были выпущены локальные акты, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в отношении персональных данных.

Разработка политики осуществлена с целью обеспечения защиты прав и свобод субъекта персональных данных при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2.2. Работа с Linux

В процессе прохождения практики была рассмотрена российская операционная система (далее - ОС) "РЕД ОС" в настоящее время актуальная по вопросам национальной безопасности и запрета использования иностранного программного обеспечения (постановление правительства от 16 ноября № 1236).

РЕД ОС – это операционная система на базе ядра Linux, построенная на решениях с открытым исходным кодом. Отечественный продукт подходит для использования на рабочей станции или для развертывания сервера. Операционная система была занесена в Единый реестр российский программ 23 июля 2017 года.

В первую очередь для установки РЕД ОС была создана виртуальная машина в VirtualBox и настроены сетевые адаптеры. Это изображено на рисунке 1.

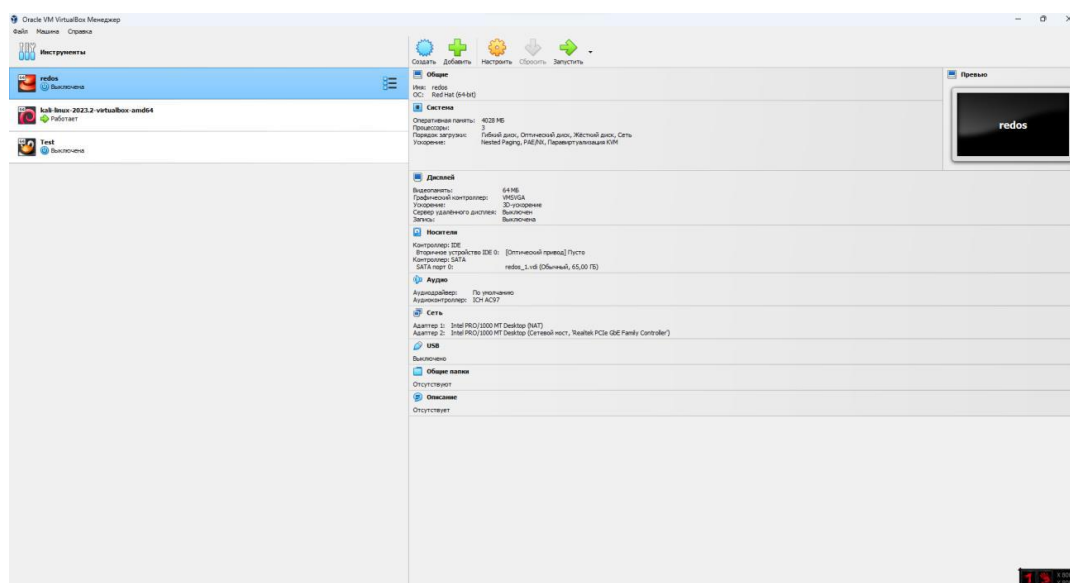


Рисунок 1 – Настройка виртуальной машины РЕД ОС

На виртуальной машине подключено 2 сетевых адаптера: NAT и сетевой адаптер, чтобы была возможность выйти в интернет и объединить в сеть два устройства. Для работы операционной системы было выделено от процессора 3 ядра и 4 ГБ оперативной памяти.

Далее, на рисунке 2 продемонстрирована уже установленная операционная система РЕД ОС и подробная информация о ней.

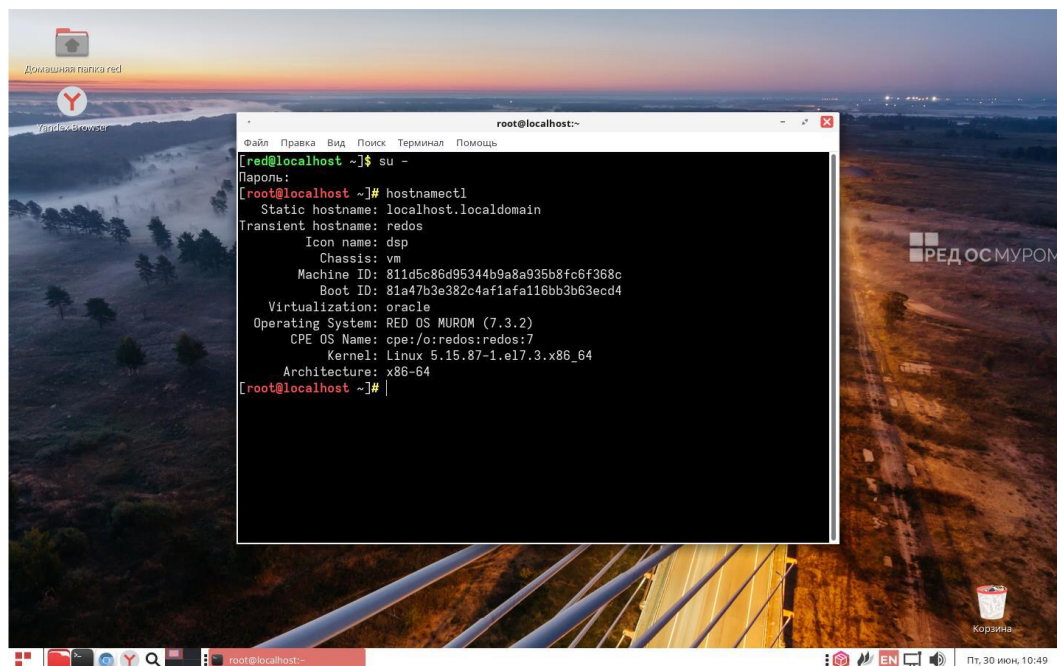


Рисунок 2 – Подробная информация по системе

Следующий этап – это установка веб-сервера Apache и её полная настройка в системе для автоматического запуска (изображено на рисунке 3).

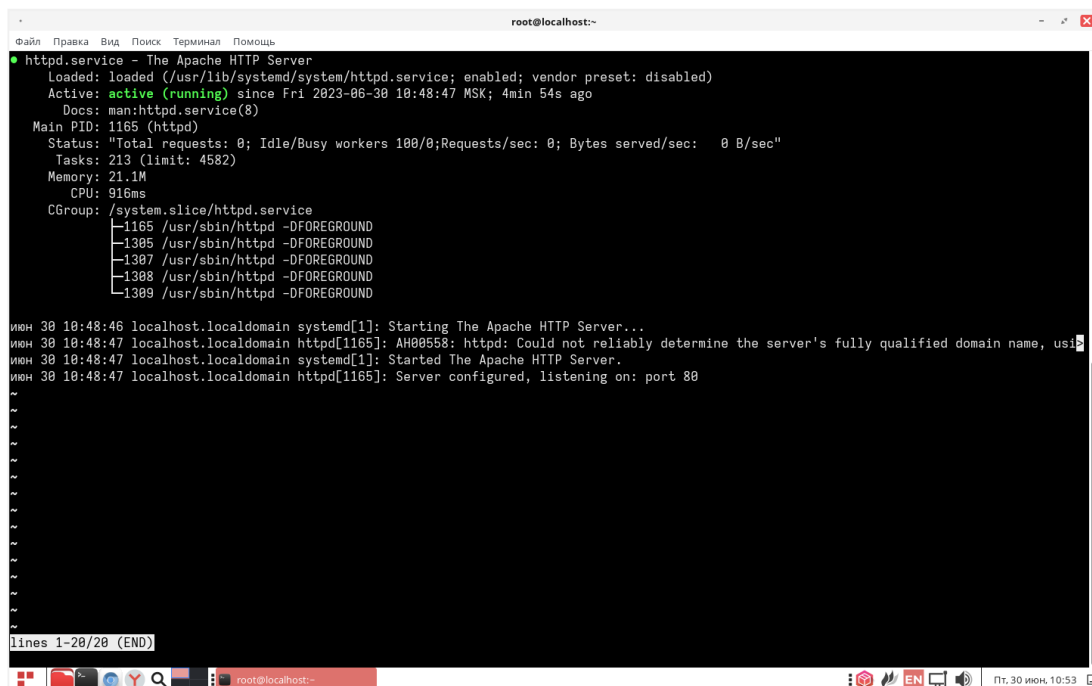


Рисунок 3 – Установка и настройка веб-сервера Apache

Используя инструмент netdiscover в ранее установленной машине KaliLinux, была просканирована локальная сеть. В результате был найден IP-адрес машины РЕД ОС – на рисунке 4.

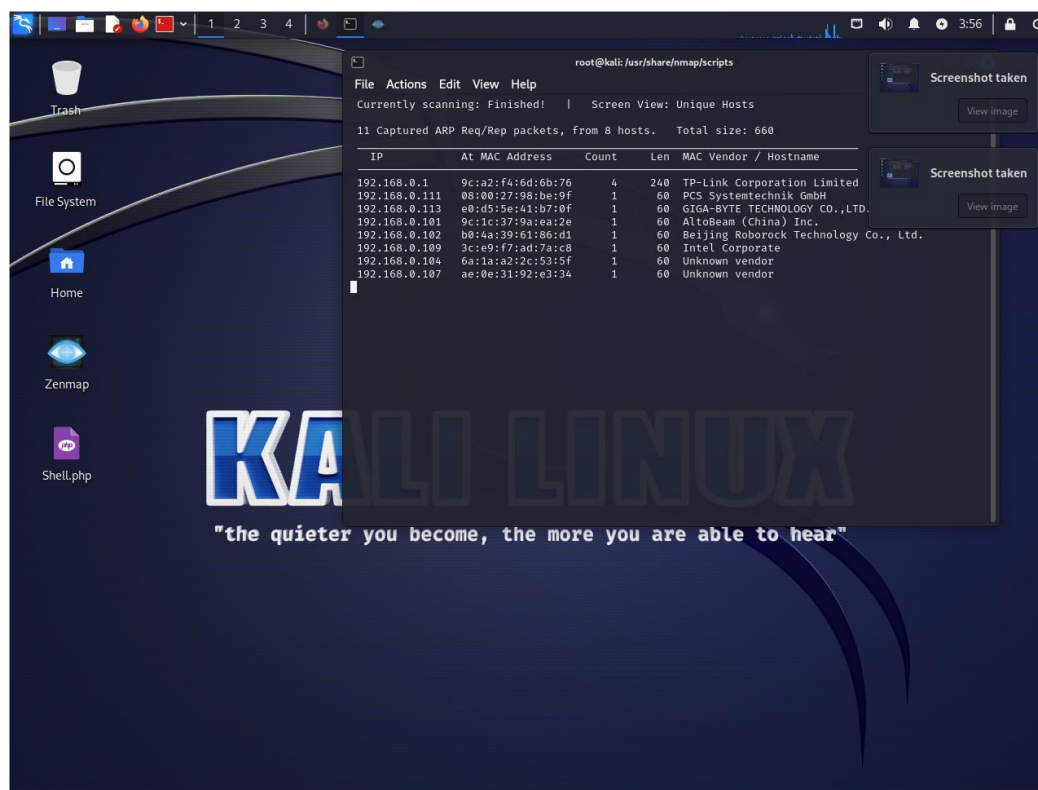


Рисунок 4 – Сканирования локальной сети в KaliLinux

При помощи утилиты zenmap было произведено сканирование сети машины РЕД ОС. На рисунке 5.1 показан процесс полного сканирования сети (Intense scan) по ранее найденному IP-адресу, а на рисунке 5.2 выведен полный список открытых портов машины РЕД ОС.

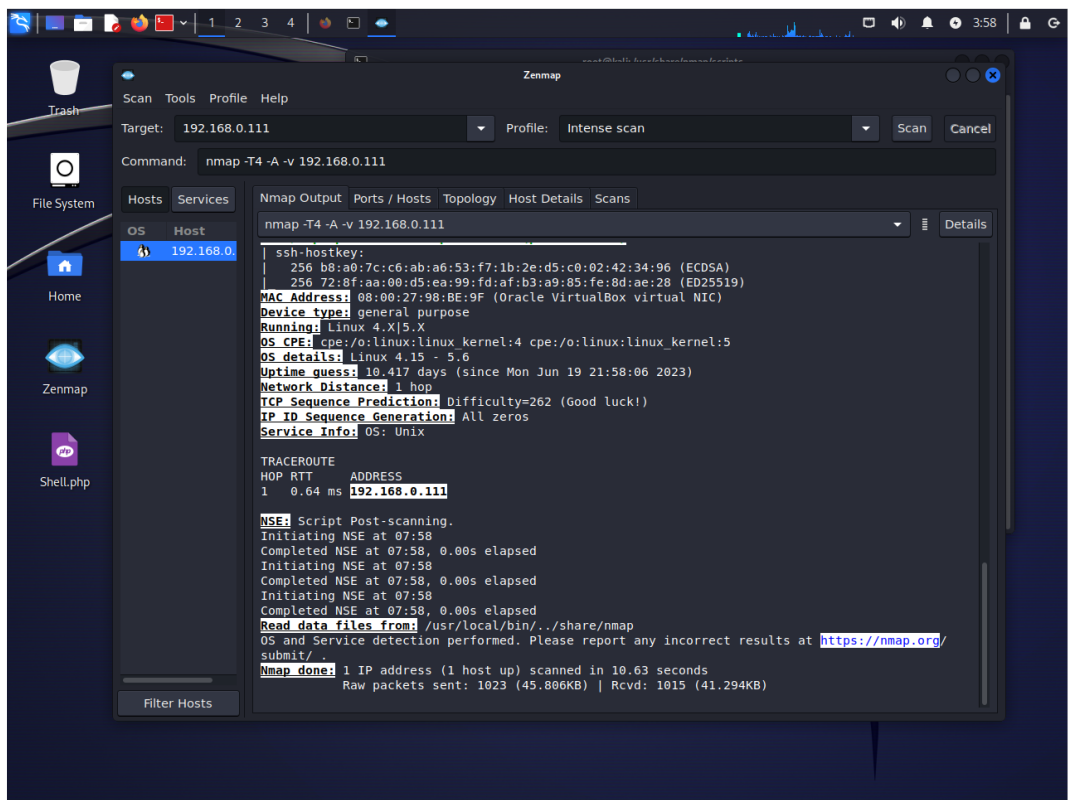


Рисунок 5.1 – Полное сканирование

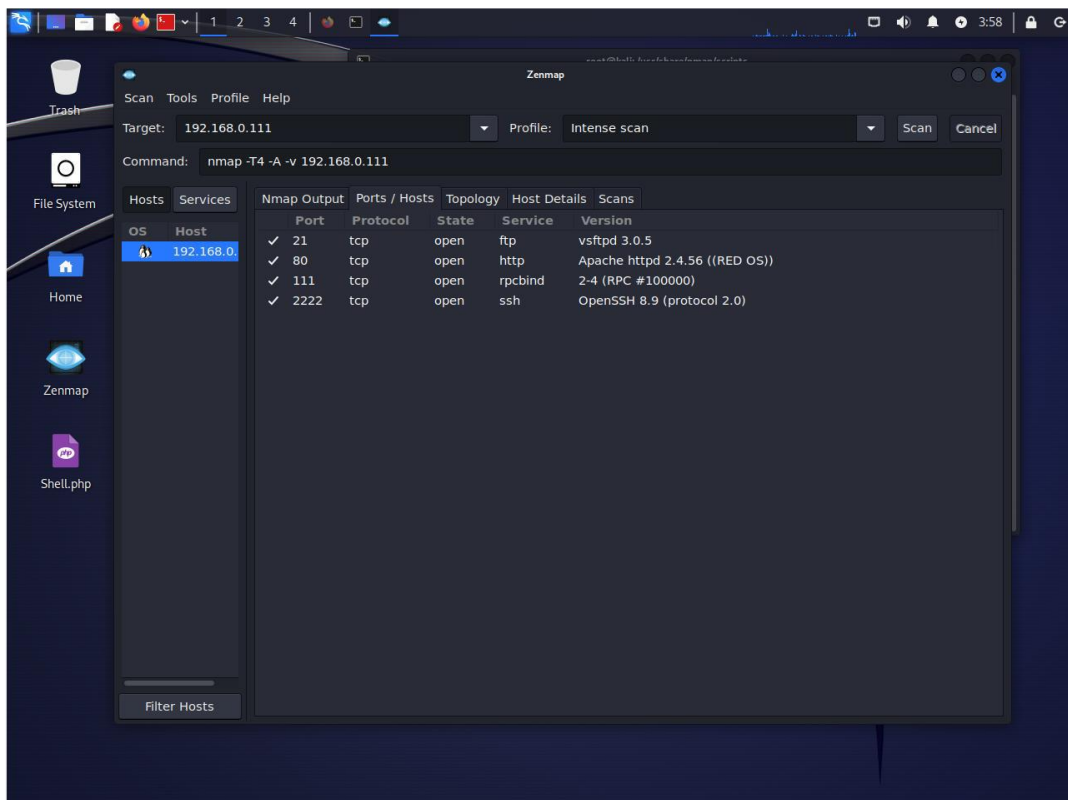
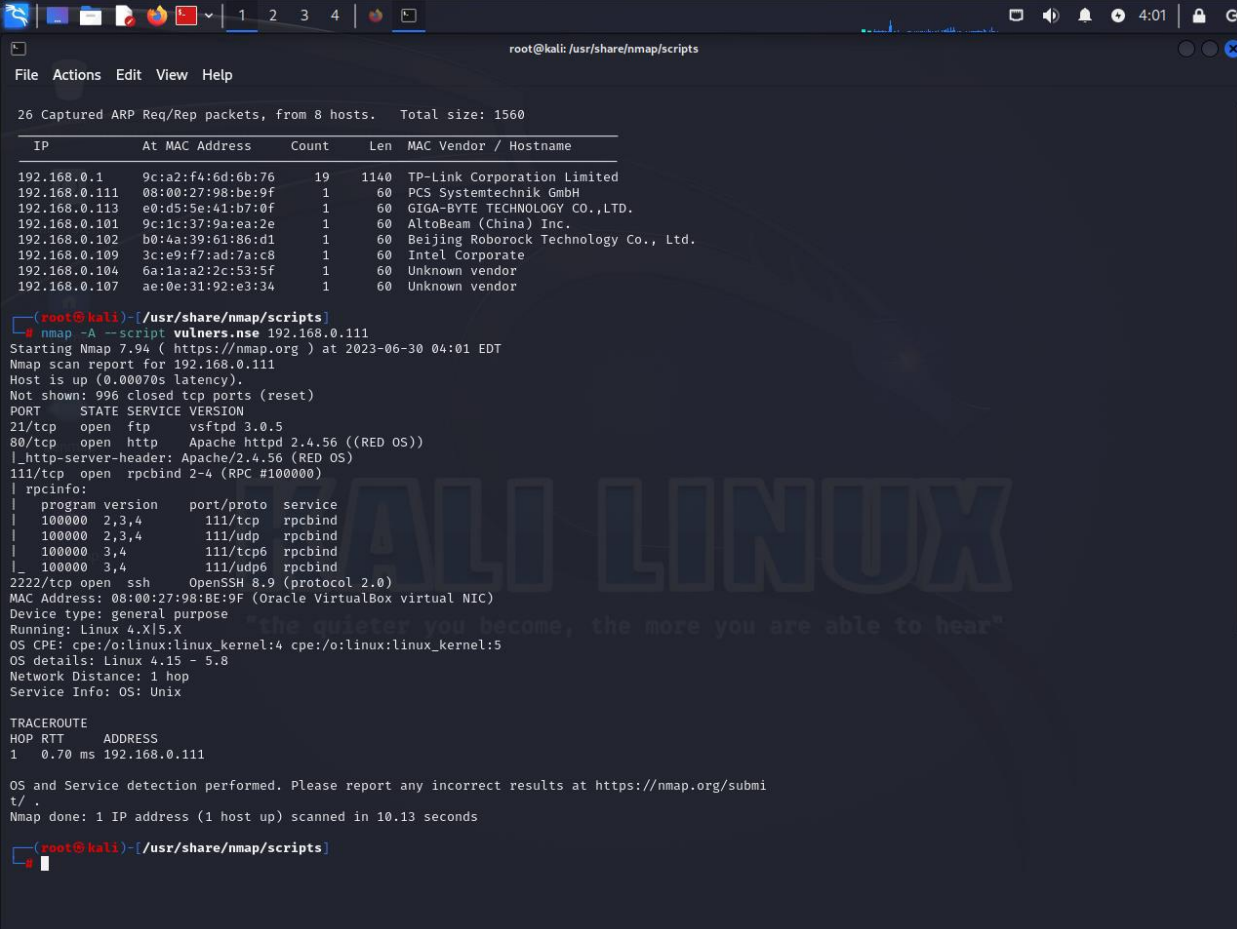


Рисунок 5.2 – Поиск открытых портов РЕД ОС

Завершающем этапом было сканирование системы с помощью *ntar*-а и скрипта *vulners.nse* для поиска уязвимостей – рисунок 6.



```
root@kali: /usr/share/nmap/scripts
File Actions Edit View Help

26 Captured ARP Req/Rep packets, from 8 hosts. Total size: 1560



| IP            | At                | MAC Address | Count | Len                                   | MAC Vendor / Hostname |
|---------------|-------------------|-------------|-------|---------------------------------------|-----------------------|
| 192.168.0.1   | 9c:a2:f4:6d:6b:76 | 19          | 1140  | TP-Link Corporation Limited           |                       |
| 192.168.0.111 | 08:00:27:98:be:9f | 1           | 60    | PCS Systemtechnik GmbH                |                       |
| 192.168.0.113 | e0:d5:5e:41:b7:0f | 1           | 60    | GIGA-BYTE TECHNOLOGY CO.,LTD.         |                       |
| 192.168.0.101 | 9c:1c:37:9a:ea:2e | 1           | 60    | AltoBeam (China) Inc.                 |                       |
| 192.168.0.102 | b0:4a:39:61:86:d1 | 1           | 60    | Beijing Roborock Technology Co., Ltd. |                       |
| 192.168.0.109 | 3c:e9:f7:ad:7a:c8 | 1           | 60    | Intel Corporate                       |                       |
| 192.168.0.104 | 6a:1a:a2:2c:53:5f | 1           | 60    | Unknown vendor                        |                       |
| 192.168.0.107 | ae:0e:31:92:e3:34 | 1           | 60    | Unknown vendor                        |                       |



(root@kali)-[/usr/share/nmap/scripts]
# nmap -A --script vulners.nse 192.168.0.111
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-30 04:01 EDT
Nmap scan report for 192.168.0.111
Host is up (0.00070s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
80/tcp    open  http     Apache httpd 2.4.56 ((RED OS))
|_http-server-header: Apache/2.4.56 (RED OS)
111/tcp   open  rpcbind  2-4 (RPC #100000)
|_rpcinfo:
|_  program version port/proto service
|_  100000  2,3,4    111/tcp    rpcbind
|_  100000  2,3,4    111/udp    rpcbind
|_  100000  3,4      111/tcp6   rpcbind
|_  100000  3,4      111/udp6   rpcbind
2222/tcp  open  ssh      OpenSSH 8.9 (protocol 2.0)
MAC Address: 08:00:27:98:BE:9F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT ADDRESS
1 0.70 ms 192.168.0.111

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 10.13 seconds

(root@kali)-[/usr/share/nmap/scripts]
```

Рисунок 6 – Поиск уязвимостей с помощью *ntar*

В результате сканирования машины РЕД ОС при помощи команды *ntar -A --script vulners.nse* уязвимости не были обнаружены, поскольку веб-сервер, поставленные на машину, последней версии – там уязвимости не обнаруживаются.

ЗАКЛЮЧЕНИЕ

По завершению прохождения производственной практики мной было приобретено значительное количество навыков по защите информации, как с технической точки зрения, так и с организационной. Полученные на практике навыки могут быть применимы в дальнейшей деятельности.

Мной в полном объеме выполнены все поставленные руководителем организации поручения, а также задачи производственной практики. Я овладел необходимыми практическими навыками, усвоил и закрепил более углубленные теоретические и юридические познания.

СПИСОК ЛИТЕРАТУРЫ

1. Прохорова О. В. Информационная безопасность и защита информации: учебник для вузов / О.В.Прохорова. – 4е изд., стер. – Санкт-Петербург: Лань, 2022. — 124 с. – ISBN 978-5-507-44201-0
2. Таненбаум Э., Уэзеролл Д. T18 Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.: ил. ISBN 978-5-459-00342-0
3. Письмо Министерства здравоохранения РФ от 7 декабря 2015 г. N 13-2/1538 "О сроках хранения медицинской документации"
4. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» // Собрание законодательства РФ. – 2006.
5. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 25.02.2022) (с изм. и доп., вступ. в силу с 01.03.2022) [Электронный ресурс] — URL: http://www.consultant.ru/document/cons_doc_law_34683/
6. Командная строка Linux. Полное руководство. — СПб.: Питер, 2017. — 480 с.: ил. — (Серия «Для профессионалов»). ISBN 978-5-496-02303-0
7. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. -М.: Горячая линия - Телеком, 2006. - 544 с.: ил. ISBN 5-93517-292-5.