Лабораторная работа 2

**Настройка лабораторного стенда**

## **Задача**

Настроить ВМ для функционирования ELK SIEM

## **Общие сведения и сценарии**

В ходе данной лабораторной работы студенты научатся запускать docker контейнеры, а также настраивать клиентские устройства, для отправки логов в Elasticsearch.

## **Необходимые ресурсы**

ПК или ноутбук с доступом к Интернету и настроенным лабораторным стендом.

## Ход выполнения лабораторной работы

### Шаг 1 - Настройка ВМ Server

Для работы с данной виртуальной машиной первостепенно необходимо настроить сеть.

1.1 Настройка сети

1.1.1 Запускаем Server, после чего входим в учетную запись при помощи логина и пароля, заданного в прошлой лабораторной работе, и переходим в режим суперпользователя с помощью команды:

#su -

1.1.2 Вводим команду ip addr и смотрим название сетевого интерфейса (кроме lo).

1.1.3 Вводим команду ls /etc/sysconfig/network-scripts и проверяем, что там присутствует файл ifcfg-<ваш интерфейс>, например ifcfg-enp0s3

1.1.4 Открываем данный файл вашим текстовым редактором, например, nano /etc/sysconfig/network-scripts/ifcfg-enp0s3

1.1.5 Добавляем новые параметры IPADDR и NETMASK со значениями 192.168.128.50 и 255.255.255.0 соответсвенно. Изменяем значение BOOTPROTO на none, а также отключаем ipv6. Итоговая конфигурация должна быть как на рисунке 1

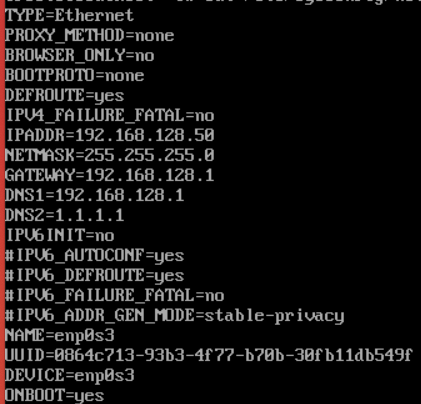


Рис. 1. Конфигурация сети для ВМ Server

1.1.6 Конфигурируем файл /etc/sysconfig/network в соответствии с рисунком 2

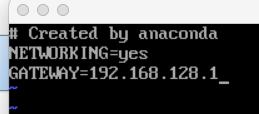


Рис. 2. Конфигурация сети для ВМ Server

1.1.7 Добавляем DNS сервера в файл /etc/resolv.conf, например 1.1.1.1 и 192.168.128.1 (Рисунок 3)

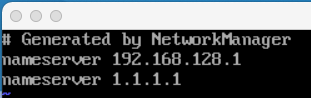


Рис. 3. Конфигурация сети для ВМ Server

1.1.8 Финальным этапом будет вызов команды для перезагрузки сетевого сервиса: systemctl restart network.

1.1.9 С помощью команды systemctl status network убедимся в том, что сервис успешно перезапустился (Рисунок 4)

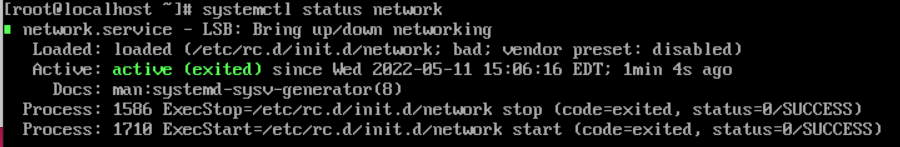


Рис. 4. Конфигурация сети для ВМ Server

1.1.10 Команда ping поможет нам проверить работоспособность нашей конфигурации, для этого введите: ping google.com

Далее все команды приведенные ниже можно выполнять из окна ВМ Server, однако для удобства лучше использовать ssh подключение к нему (так появляется возможность копировать команды и вставлять их). Для этого необходимо установить openssh-server.

1.2 Установка openssh-server

1.2.1 Запускаем Server, после чего входим в учетную запись при помощи логина и пароля, заданного в прошлой лабораторной работе.

1.2.2 Переходим в режим суперпользователя: su -

1.2.3 Обновляем систему с помощью команды: yum update -y

1.2.4 Устанавливаем openssh-server: yum -y install openssh-server openssh-client

1.2.5 Запускаем сервис sshd: systemctl start sshd

1.2.6 Проверяем работоспособность сервиса: systemctl status sshd (Рисунок 5)

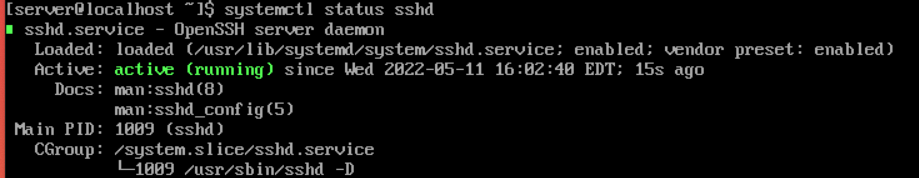


Рис. 5. Статус сервиса sshd

1.2.7 Подключаемся по ssh к ВМ Server с помощью команды: ssh -p 122 server@localhost (Рисунок 6)

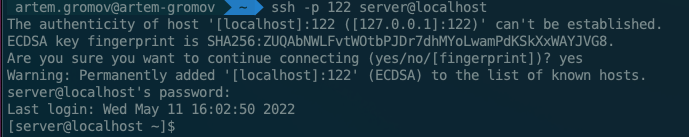


Рис. 6. Успешное подключение по ssh

1.3 Установка docker

1.3.1 Устанавливаем docker с помощью пакетного менеджера:

yum install -y yum-utils

yum-config-manager --add-repo <https://download.docker.com/linux/centos/docker-ce.repo>

yum install docker -y

systemctl start docker

systemctl enable docker

docker run hello-world

Если все прошло успешно, должно появиться следующее сообщение (Рисунок 7)

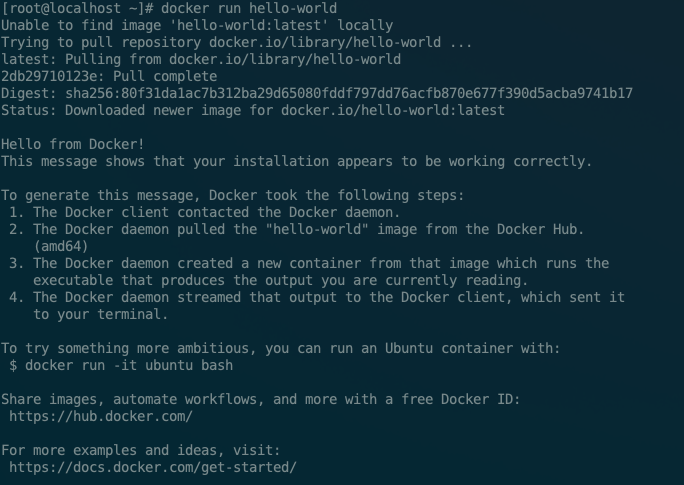


Рис. 7. Вывод команды docker run hello-world

1.4 Установка docker-compose

1.4.1 Для установки docker-compose необходимо ввести следующие команды:

curl -L "https://github.com/docker/compose/releases/download/1.26.2/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose

chmod +x /usr/local/bin/docker-compose

1.5 Установка git

1.5.1 Ввести команду: yum install git

1.6 Запуск ELK Stack

1.6.1 Для запуска Elasticsearch и Kibana необходимо клонировать следующий репозиторий с помощь следующей команды: git clone [https://AA122AA/elk\_siem\_labs](https://aa122aa/elk_siem_labs)

1.6.2 Переходим в папку lab\_2 с помощью команды: cd elk\_siem\_labs/lab\_2

1.6.3 Далее необходимо перейти к файлу /etc/selinux/config и внести следующие изменения в файл (Рисунок 8)

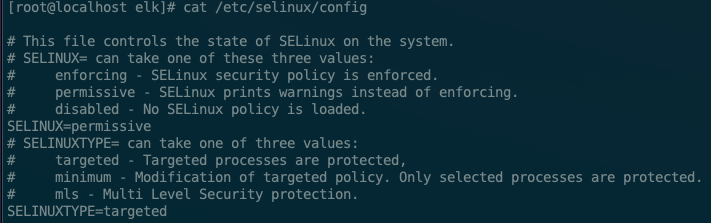


Рис. 8. Изменения в файле /etc/selinux/config

1.6.4 Перезагружаем систему командой reboot

1.6.5 Запускаем ELK Stack с помощью команды docker-compose up --build -d и ждем примерно минуту

1.6.5 Необходимо создать пароли для внутренних пользователей с помощью следующей команды: docker-compose exec elasticsearch /usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto

1.6.6 Копируем пользователя elastic и его пароль в /kibana/config/kibana.yml (Рисунок 9)

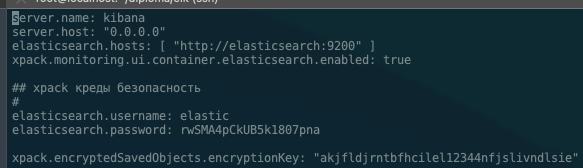


Рис. 9. Добавляем данные пользователя elastic

1.6.7 Перезапускаем ELK Stack с помощью команды: docker-compose restart

1.6.8 Переходим по сслыке <http://localhost:5601>. Для входа в интерфейс Kibana необходимо ввести те же данные, что и в файле.

### Шаг 2 - Настройка ВМ Client

2.1 Настройка сети

Настройка сети происходит аналогично пункту 1.1 с единственной поправкой - IP адрес необходимо заменить на 192.168.128.51. Итоговый файл конфигурации должен выглядеть, как на рисунке 10

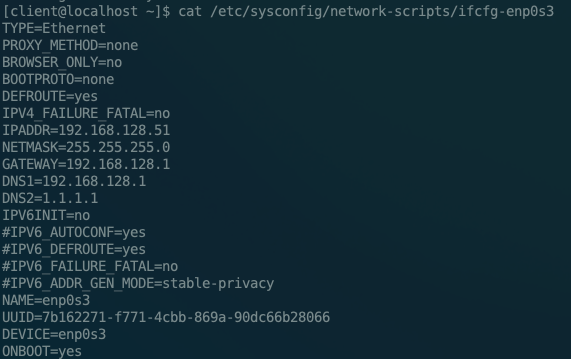


Рис. 10. Конфигурация файла /etc/sysconfig/network-scripts/ifcfg-enp0s3

2.2 Установка openssh-server

Установка и настройка ssh происходит аналогично пункту 1.2 с единственным изменением: подключение происходит с помощью следующей команды ssh -p 222 client@localhost

2.3 Установка Filebeat

2.3.1 Передать файл filebeat\* на ВМ Client с помощью команды: scp -P 222 filebeat\* client@localhost:~/

Примечание: Если ваша ОС Windows, для этого действия вам необходимо использовать консольную утилиту pscp и команду: pscp -scp -P 222 filebeat\* client@localhost:~/

2.3.2 Подключиться с помощью ssh к виртуальной машине Client: ssh -p 222 client@localhost

2.3.3 Убедиться, что файл передался с помощью команды: ls (Рисунок 11)



Рис. 11. Filebeat присутствует на ВМ Client

2.3.4 Перейти в режим суперпользователя: su

2.3.5 Установить программу с помощью команды: rpm -vi filebeat-7.16.2-x86\_64.rpm

2.3.6 Перейти к редактирования файла конфигурации: nano /etc/filebeat/filebeat.yml

2.3.6.1 Настроить раздел “Outputs” как показано на рисунке 12, указав пароль, полученный в прошлом шаге

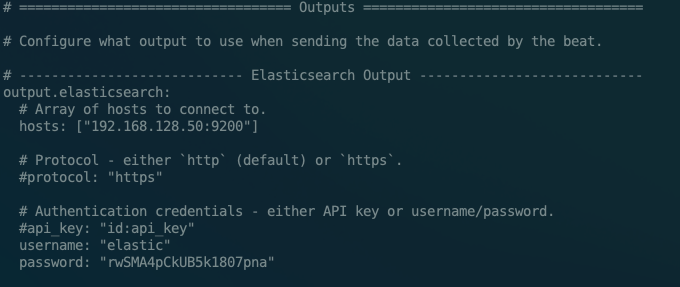


Рис. 12. Раздел “Outputs”

2.3.6.2 Настроить раздел “Kibana” как показано на рисунке 13

setup.kibana.host: "192.168.128.50:5601"

setup.kibana.ssl.enable: false

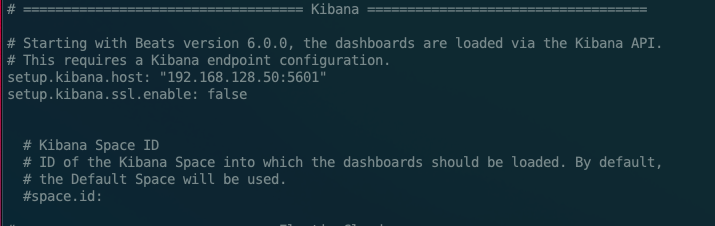


Рис. 13. Раздел “Kibana”

2.3.6.3 Настроить раздел “Filebeat inputs” как показано на рисунке 14

enabled: true

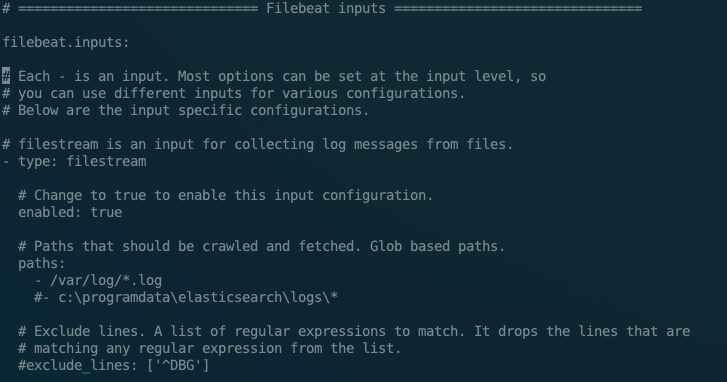


Рис. 14. Раздел “Filebeat inputs”

2.3.6.3 Настроить раздел “Elasticsearch template setting” как показано на рисунке 15

setup.ilm.enabaled: true

setup.ilm.overwrite: true

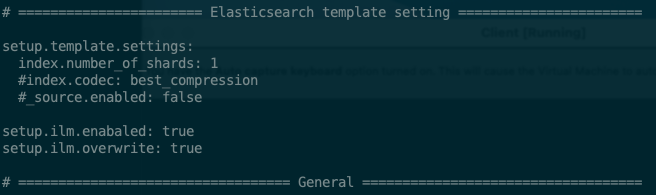


Рис. 15. Раздел “Elasticsearch template setting”

2.3.7 Для того чтобы применить внесенные изменения необходимо ввести команду: filebeat setup -e

2.3.8 Запускаем Filebeat: service filebeat start

Перейдя на вкладку “Discover” в интерфейсе Kibana (Рисунок 16), надо выбрать временной период за последний год (Рисунок 17).

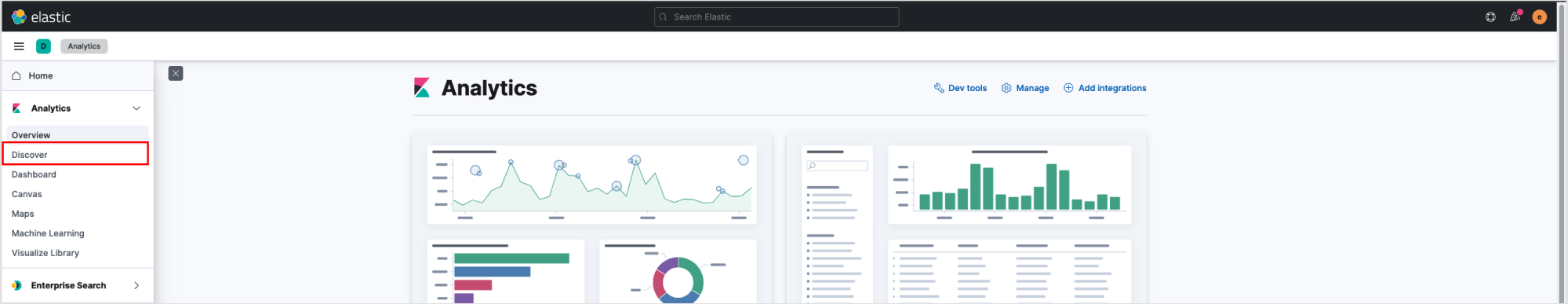


Рис. 16. Переход к вкладке “Discover”

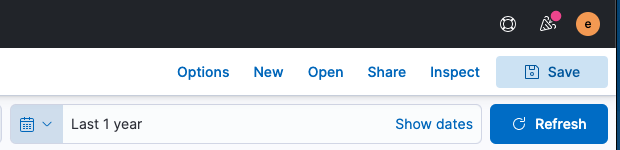


Рис. 17. Изменение временного периода

Результат выполнения шага 2 представлен на рисунке 18

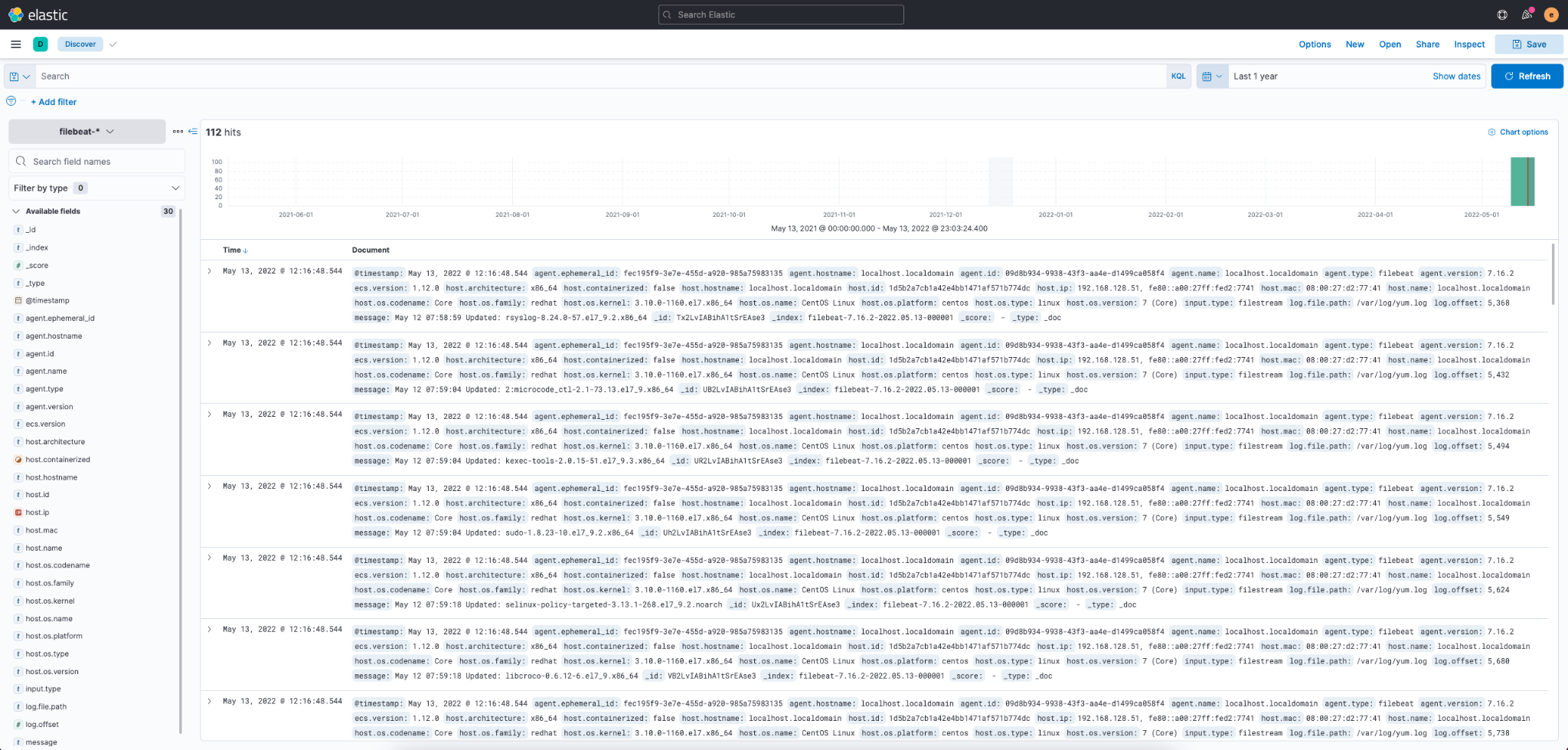


Рис. 18 Лог-файлы устройства под управлением CentOs

### Шаг 3 - Настройка ВМ Windows 7

Для удобства работы рекомендуется установить “Гостевые дополнения".

3.1 Настройка сети

3.1.1 Для настройки статической маршрутизации в Windows 7 необходимо перейти в “Панель управления” -> ”Сеть и Интернет” -> ”Центр управления сетями и общим доступом” -> ”Изменение параметров адаптера” -> ”Подключение по локальной сети” -> ”Свойства” -> ”Протокол интернета версии 4” -> ”Использовать следующий IP адрес”. Затем ввести данные представленные на рисунке 19. После применения изменений в появившемся окне выбрать “Домашняя сеть”.

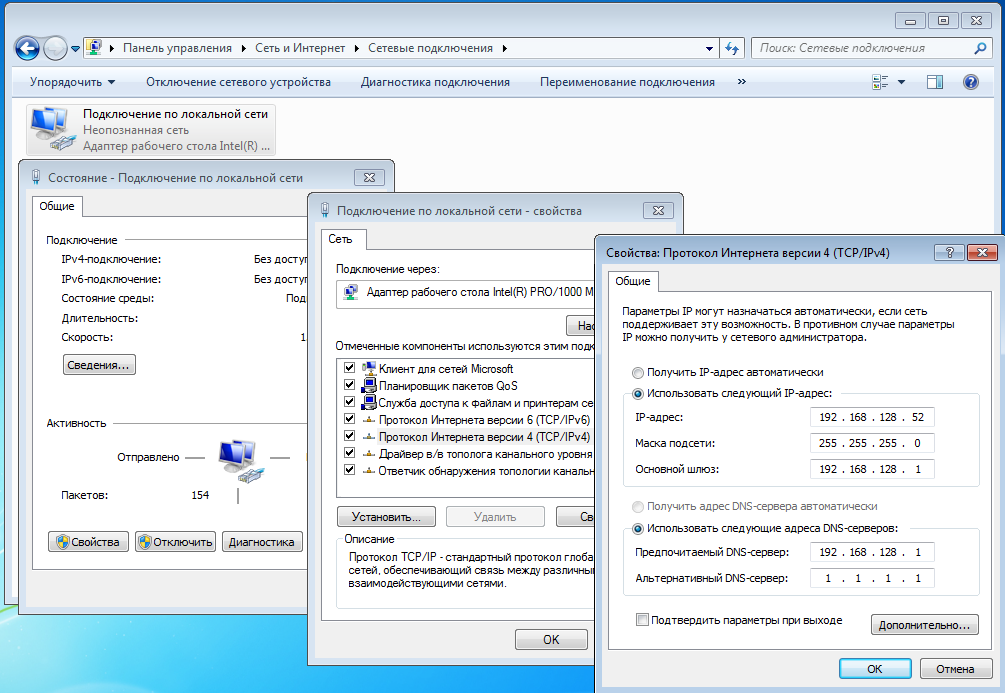


Рис. 19. Настройка сети

3.1.2 Отключить Брандмауэр Windows (Рисунок 20)

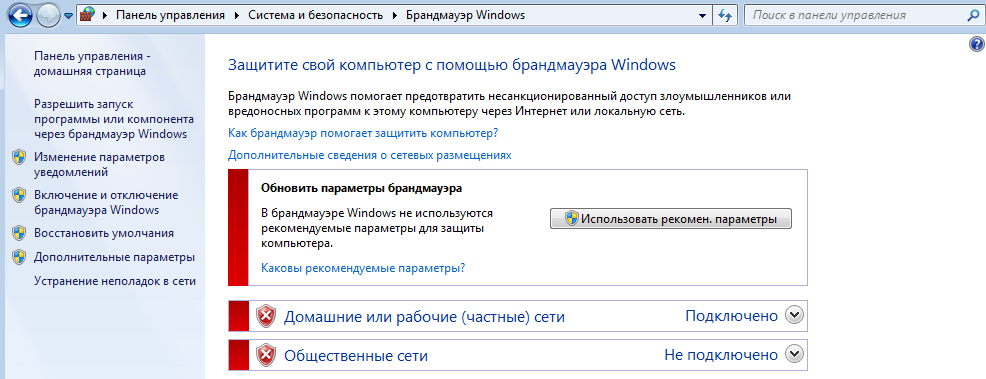


Рис. 20. Отключение брандмауэра Windows

3.2 Установка Packetbeat

3.2.1 Перенести файл packetbeat\* на рабочий стол

3.2.2 Распаковать файл в папку C:\Program Files (Рисунок 21)

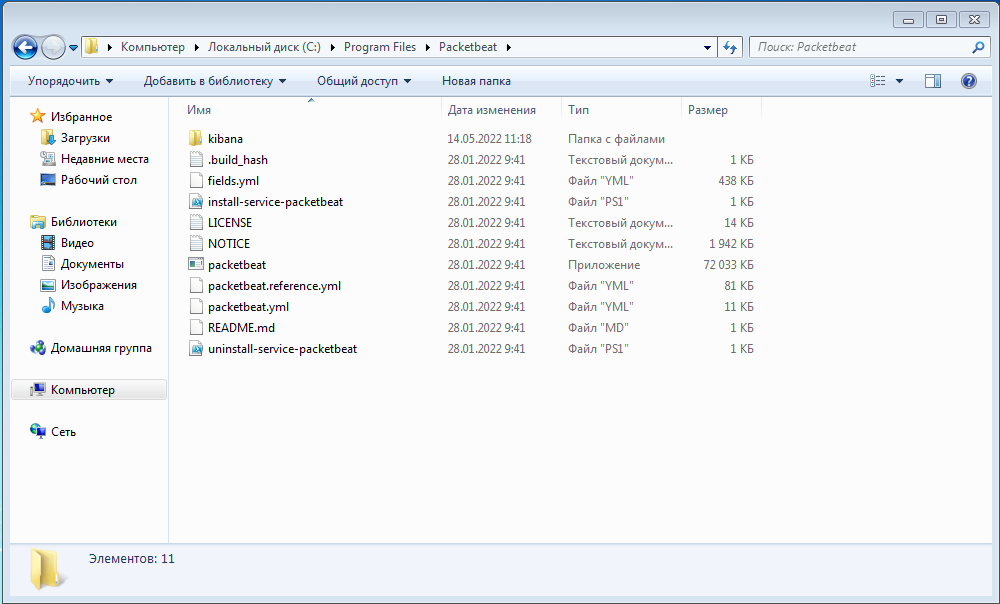


Рис. 21. Распакованный архив с программой Packetbeat

3.2.3 Для правильно работы программы необходимо установить WinPcap <https://www.winpcap.org/install/>

3.2.4 Установка Packetbeat в качестве системной службы показана на рисунке 22. Запустите PowerShell от имени администратора и введите следующие команды:

cd 'C:\Program Files\Packetbeat'

PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-packetbeat.ps1

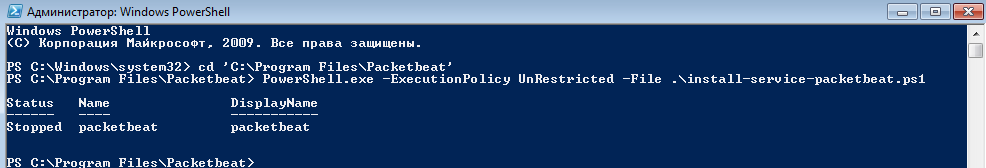


Рис. 22. Установка Packetbeat

3.2.5 Конфигурация файла packetbeat.yml

3.2.5.1 Настройка подключения к Kibana (Рисунок 23)

host: "192.168.128.50:5601"

setup.kibana.ssl.enabled: false

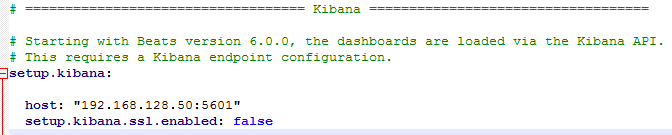


Рис. 23. Настройка раздела “Kibana”

3.2.5.2 Настройка подключения к Elasticsearch (Рисунок 24)

hosts: ["192.168.128.50:9200"]

username: "elastic"

password: "Ваш пароль"

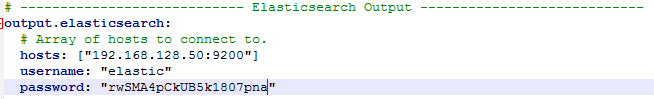


Рис. 24. Настройка раздела “Elasticsearch Output”

3.2.6 Для настройки опции packetbeat.interfaces.device, необходимо ввести следующую команду в окно программы PowerShell .\packetbeat.exe devices (Рисунок 25). В качестве значения для данной опции необходимо ввести цифру, присвоенную сетевой карте.



Рис. 25. Вывод команды .\packetbeat.exe devices

3.2.7 Для того чтобы применить внесенные изменения необходимо ввести следующую команду: .\packetbeat.exe setup -e

Введите команду Start-Service packetbeat для запуска сервиса Packetbeat. В интерфейсе Kibana, перейдя на индекс “packetbeat\*”, можно увидеть сетевые события (Рисунок 26). Если событий нет, попробуйте выполнить команду ping до любого сервера, например ping google.com.

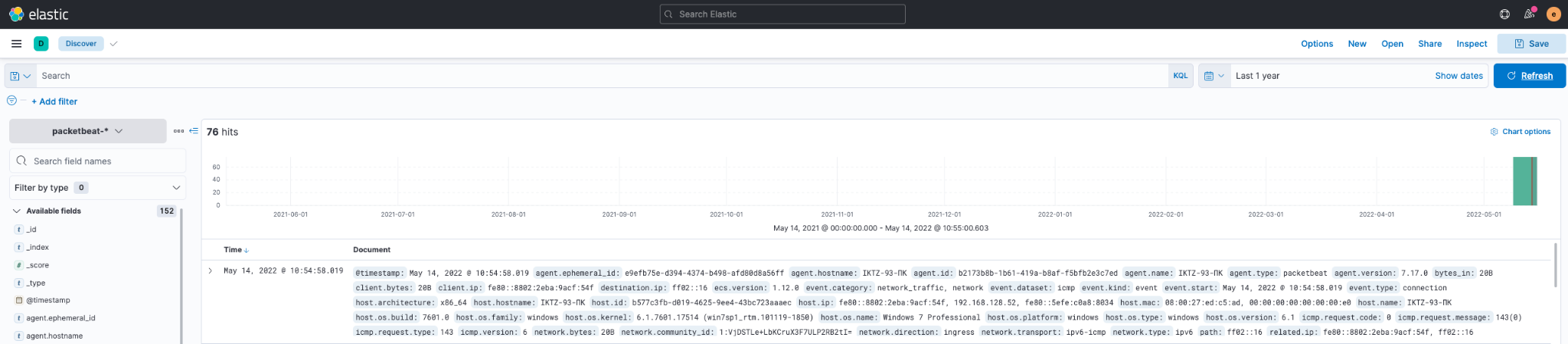


Рис. 26. События в интерфейсе Kibana

3.3 Установка Winlogbeat

3.3.1 Перенести файл winlogbeat\* на рабочий стол

3.3.2 Распаковать файл в папку C:\Program Files (Рисунок 27)

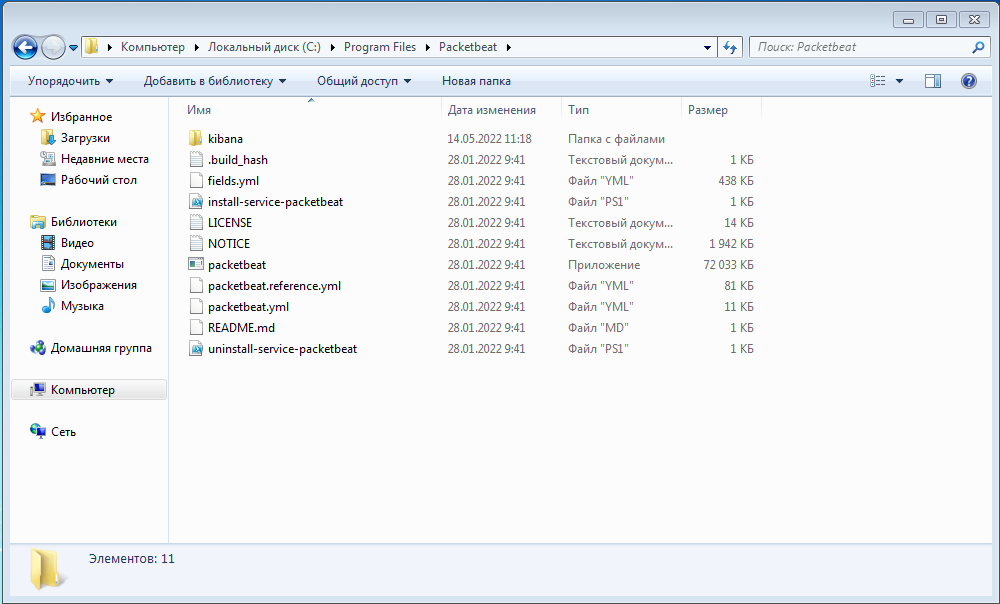


Рис. 27. Распакованный архив с программой Winlogbeat

3.3.3 Установка Winlogbeat в качестве системной службы показана на рисунке 28. Запустите PowerShell от имени администратора и введите следующие команды:

cd 'C:\Program Files\Winlogbeat

PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1

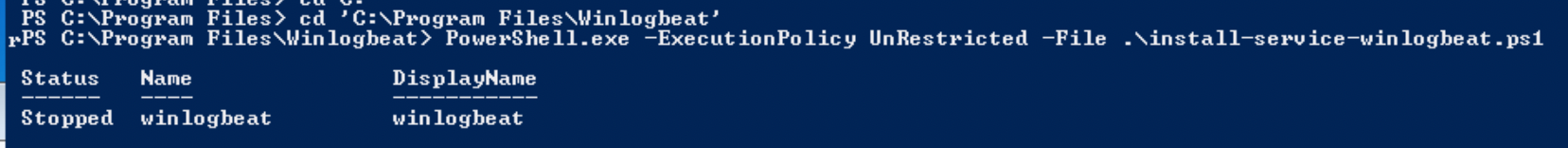


Рис. 28. Установка Winlogbeat

3.3.4 Конфигурация файла winlogbeat.yml

3.3.4.1 Настройка подключения к Kibana (Рисунок 29)

host: "192.168.128.50:5601"

setup.kibana.ssl.enabled: false

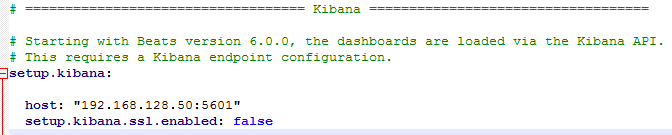


Рис. 29. Настройка раздела “Kibana”

3.3.4.2 Настройка подключения к Elasticsearch (Рисунок 30)

hosts: ["192.168.128.50:9200"]

username: "elastic"

password: "Ваш пароль"

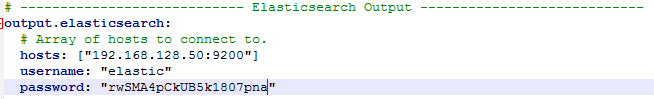


Рис. 30. Настройка раздела “Elasticsearch Output”

3.3.4.3 Для настройки получения необходимы логов добавьте следующие строчки в раздел “Winlogbeat specific options” (Рисунок 31).

- name: Microsoft-Windows-Authentication User Interface/Operational

- name: Microsoft-Windows-WMI-Activity/Operational

- name: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational

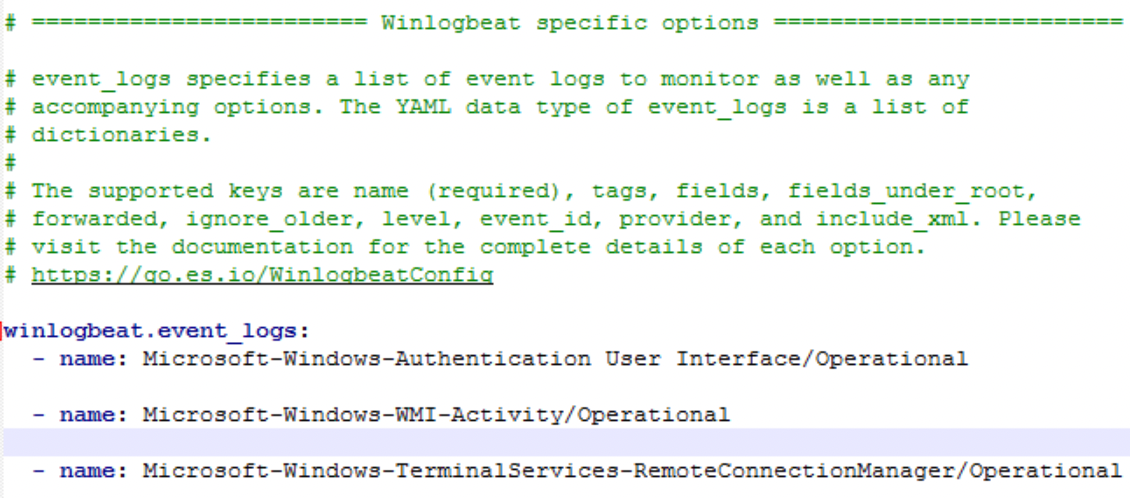


Рис. 31. Настройка дополнительных логов

3.3.5 Для того чтобы применить внесенные изменения необходимо ввести следующую команду: .\winlogbeat.exe setup -e

Введите команду Start-Service winlogbeat для запуска сервиса Winlogbeat. В интерфейсе Kibana, перейдя на индекс “winlogbeat\*”, можно увидеть windows события (Рисунок 32).

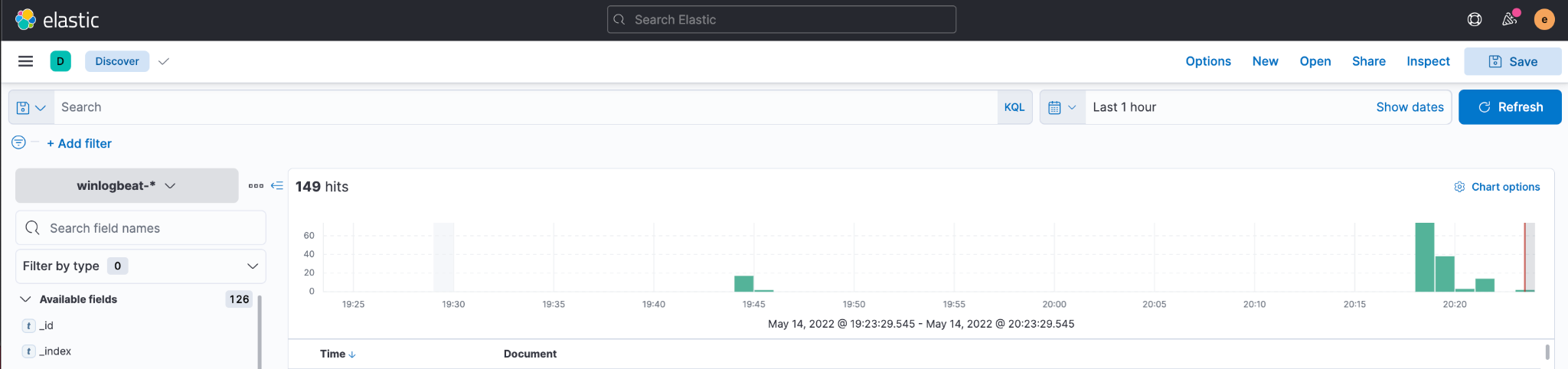


Рис. 32. События в интерфейсе Kibana

3.4 Для логирования необходимых нам событий необходимо открыть “Редактор локальной групповой политики”, введите в утилиту “Выполнить” gpedit.msc. Перейдите по следующему пути “Политика “Локальный компьютер” -> Конфигурация компьютера -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Политика аудита. (Рисунок 33). Дважды нажать на “Аудит событий входа в систему” и выбрать “Успех” и “Отказ” (Рисунок 34).

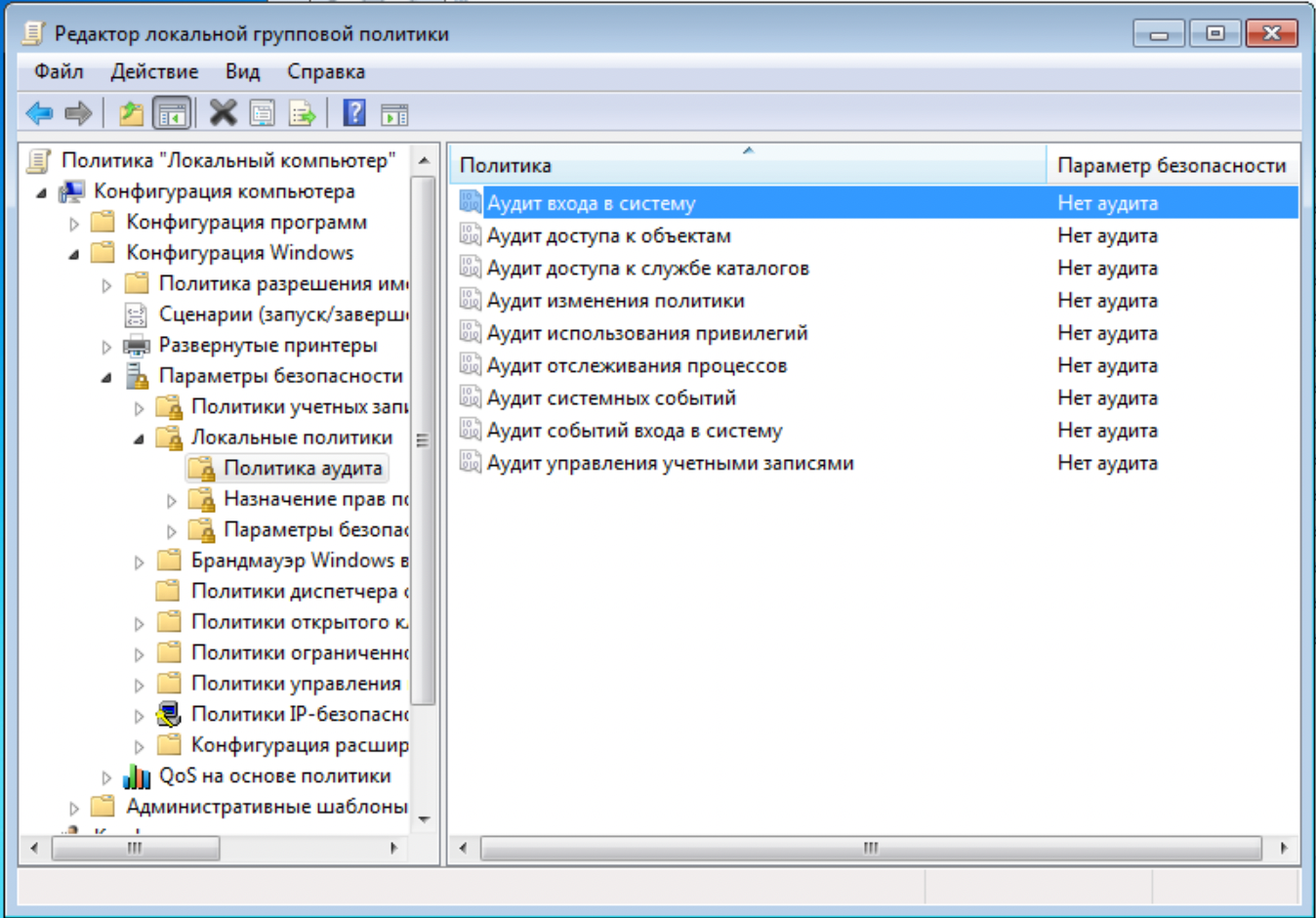


Рис. 33. Добавление необходимых событий

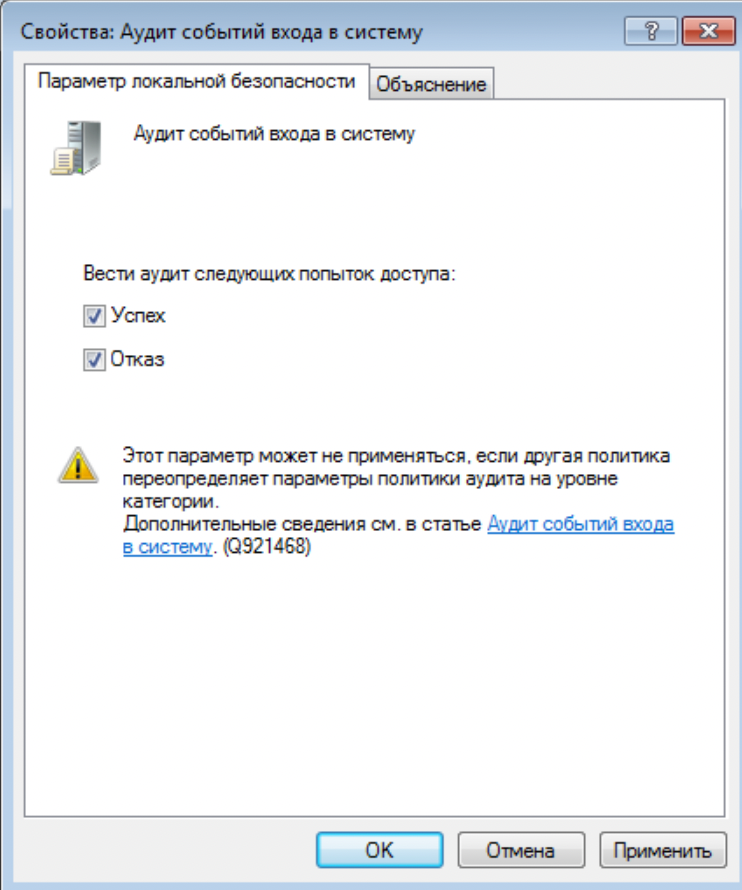


Рис. 34. Активируем события

3.5 Активация удаленного подключения по протоколу RDP

Для активации удаленного доступа по протоколу RDP необходимо перейти в “Панель управления”->”Система и безопасность”->”Настройка удаленного доступа”. Выбрать пункт “Разрешать подключение от компьютеров с любой версией рабочего стола (опаснее)” (Рисунок 35)

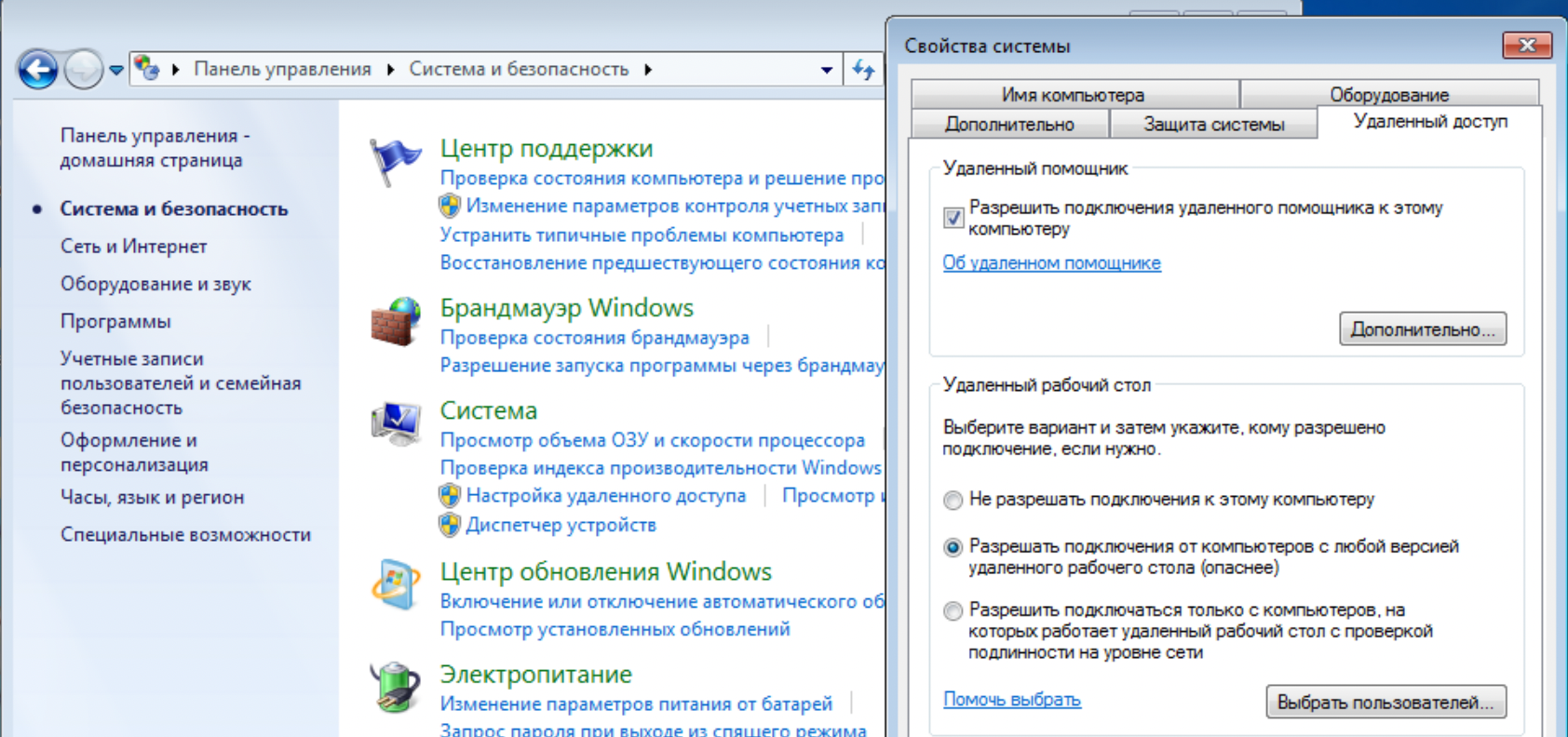


Рис. 35. Активация протокола RDP

3.6 Активация удаленного подключения по протоколу WinRM

3.6.1 Для активации службы введем следующую команду: winrm quickconfig (Рисунок 36)

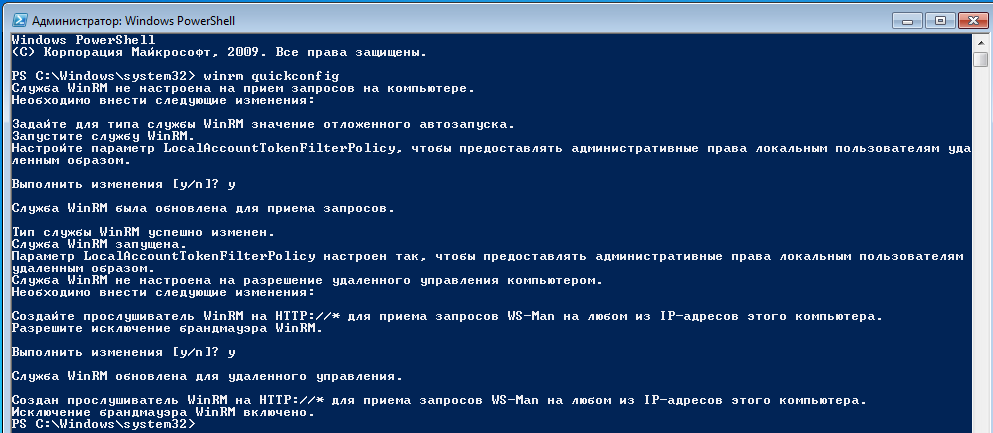


Рис. 36. Активация WinRM

3.6.2 Разрешаем авторизацию по паролю с помощью команд: winrm set winrm/config/client/auth '@{Basic="true"}', winrm set winrm/config/service/auth '@{Basic="true"}', winrm set winrm/config/service '@{AllowUnencrypted="true"}' (Рисунок 37)



Рис. 37. Разрешили авторизацию по паролю

3.6.2 Проверим работу WinRM c помощью команды: winrm e winrm/config/listener (Рисунок 38)

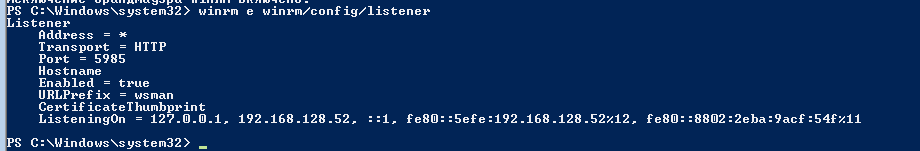


Рис. 38. Проверка работы службы WinRM

### Шаг 4 - Настройка Kali Linux

4.1 Настройка сети

4.1.1 Переходим к редактированию файла /etc/network/interfaces и вводим следующие данные (Рисунок 39):

auto eth0

iface eth0 inet static

address 192.168.128.53/24

gateway 192.168.128.1

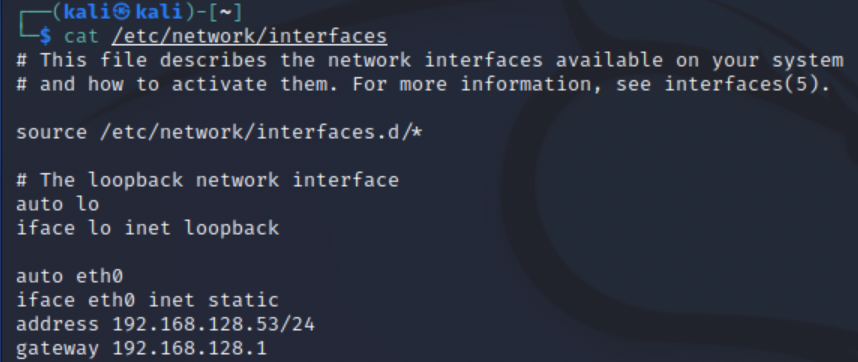


Рис. 39. Файл /etc/network/interfaces

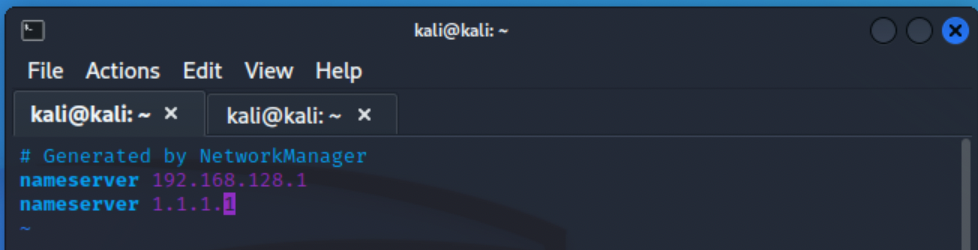
4.1.2 Добавляем DNS сервера, редактируя файл /etc/resolv.conf как показано на рисунке 40

Рис. 40. Файл /etc/resolv.conf

4.1.3 Для применения изменений необходимо ввести команду sudo service networking restart

4.2 Обновление пакетов

4.2.1 Для успешного обновления необходимо установить следующий пакет: sudo apt install libwacom-common

4.2.2 Команда для скачивания и установки обновлений: sudo apt update -y && sudo apt upgrade -y && sudo apt autoremove -y

Данный пункт может занять до 1 часа времени