**Лабораторная работа 7.**

**Nmap, Honeypot**

**Серт Серкан Группа 8**

Основные теоретические сведения

**Цель:** Получение практических и теоретических навыков работы с honeypot, способами и методами сканирования сети.

**IPv4.** В 4-й версии IP-адрес представляет собой 32-битовое число. Удобной формой записи IP-адреса (IPv4) является запись в виде четырёх десятичных чисел значением от 0 до 255, разделённых точками, например, 192.168.0.3.

**IPv6.** В 6-й версии IP-адрес (IPv6) является 128-битовым. Внутри адреса разделителем является двоеточие (напр. 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Ведущие нули допускается в записи опускать. Нулевые группы, идущие подряд, могут быть опущены, вместо них ставится двойное двоеточие (fe80:0:0:0:0:0:0:1 можно записать как fe80::1). Более одного такого пропуска в адресе не допускается

**MAC-адрес** (от англ. Media Access Control — управление доступом к среде, также Hardware Address) — уникальный идентификатор, присваиваемый каждой единице активного оборудования компьютерных сетей.

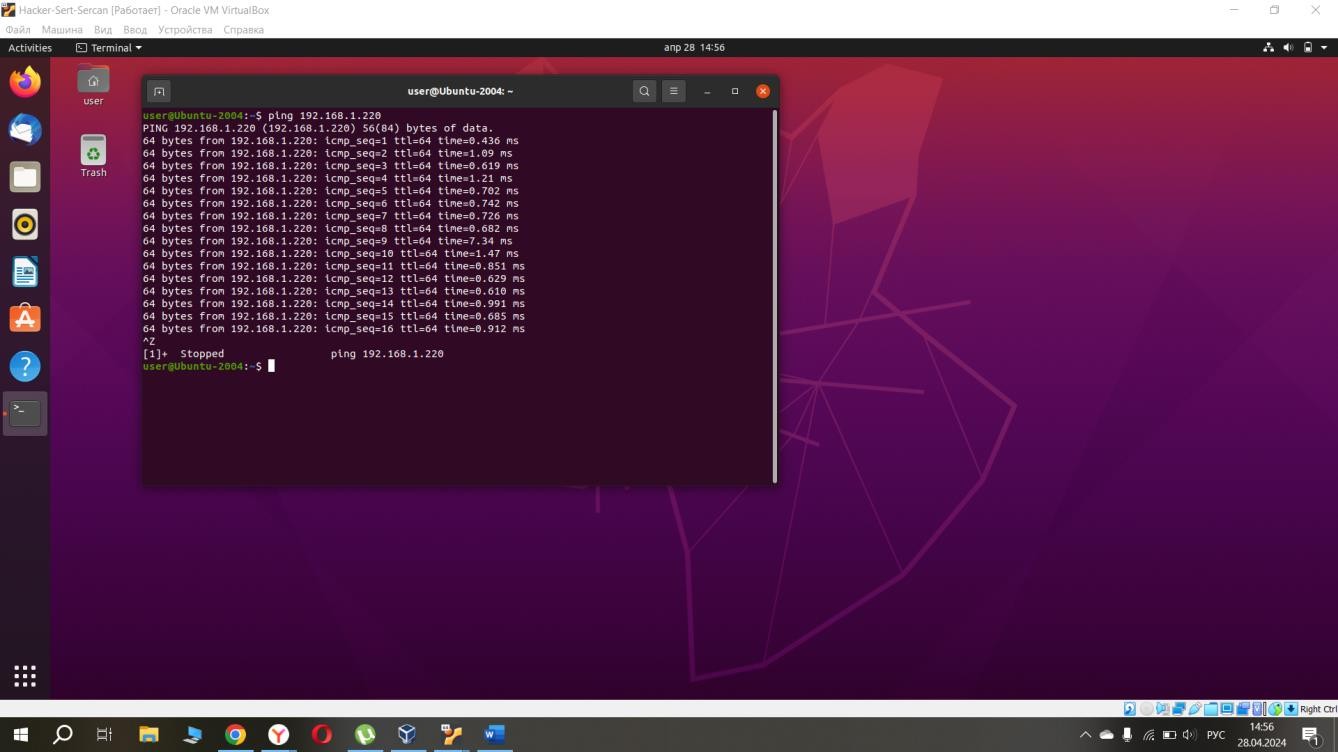
**Маска сети** - битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети (при этом, в отличие от IP-адреса, маска подсети не является частью IP-пакета). Например, узел с IP-адресом 12.34.56.78 и маской подсети 255.255.255.0 находится в сети 12.34.56.0 с длиной префикса 24 бита. В случае адресации IPv6 адрес 2001:0DB8:1:0:6C1F:A78A:3CB5:1ADD с длиной префикса 32 бита (/32) находится в сети 2001:0DB8::/32.

**DHCP** - сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

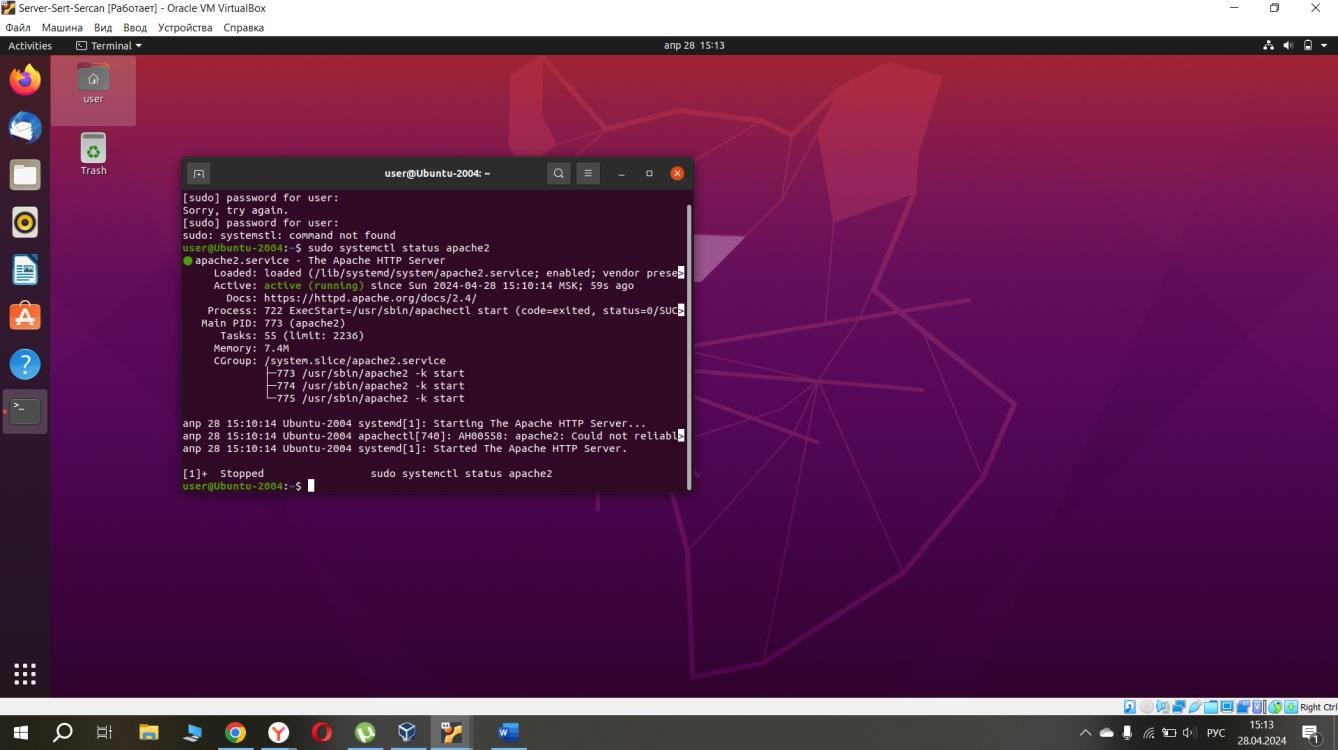
# Ping-сканирование

Самым распространенным и простым способом сканирования является простое pingсканирование, которое заключается в отправке ICMP пакетов на разные хосты. Хост, который активен, ответит на эти пакеты.

Форма подачи запроса: ping 192.168.1.220



Далее установим веб-сервер apache2 на Sever, чтобы был доступен 80й порт, предварительно перед этим необходимо выполнить команду sudo apt update, чтобы веб-сервер успешно установился.



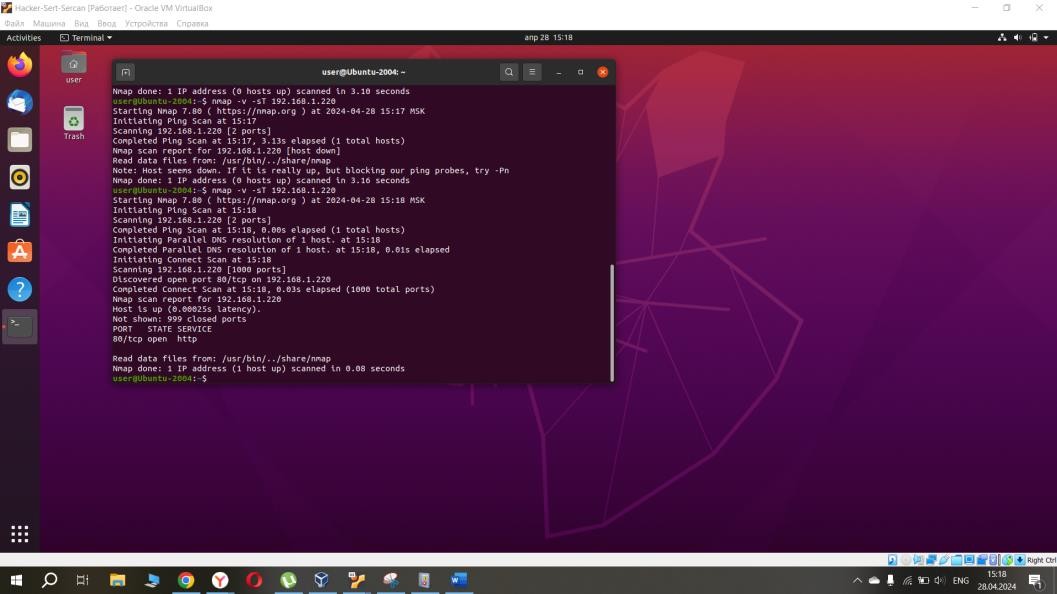
# TCP Connect()

Второй доступный метод сканирования - TCP Connect. Он заключается в том, что сканирующая машина пытается установить соединение со сканируемой. Успешный результат говорит о том, что порт открыт, неудачный — о том, что он закрыт или

фильтруется. Это сканирование легко обнаруживается по огромному количеству записей в log-файле неудачных попыток установления соединения и ошибок исполнения этой операции. Понятно, что средства защиты с максимальным быстродействием заблокируют адрес, вызывающий ошибки.

Подача запроса: nmap –sT 192.168.1.220

-v: Увеличить уровень вербальности (задать дважды или более для увеличения эффекта)

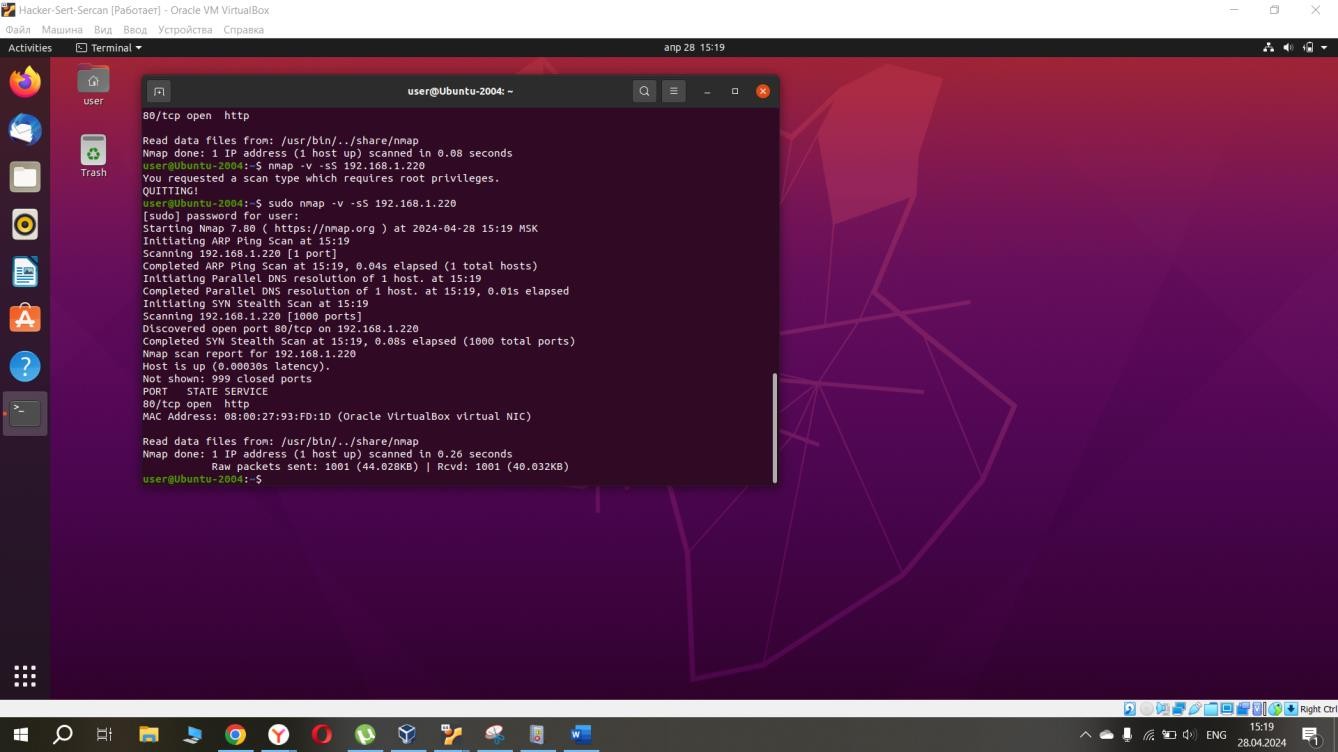


# TCP-SYN

Более совершенным методом сканирования является TCP SYN — так называемое

«полуоткрытое сканирование». При вызове Nmap посылает SYN-пакет, как бы ради того, чтобы установить новое соединение. Если в ответе присутствуют флаги SYN или ACK, считается, что порт открыт. Флаг RST говорит об обратном. Если пришел ответ, говорящий о том, что порт открыт, nmap незамедлительно отправляет RST-пакет для сброса еще не установленного соединения. Сканирование осуществляется только при наличии прав суперпользователя (root).

sudo nmap –sS 192.168.1.220

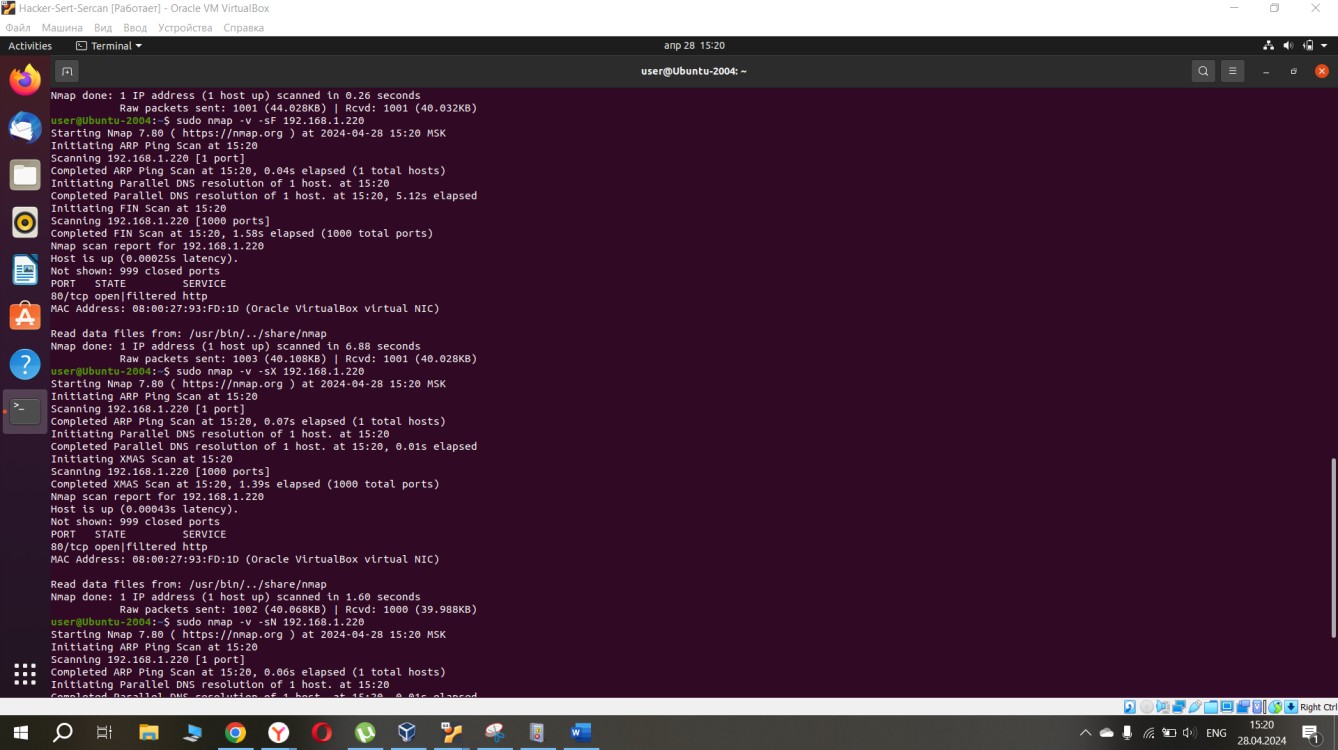


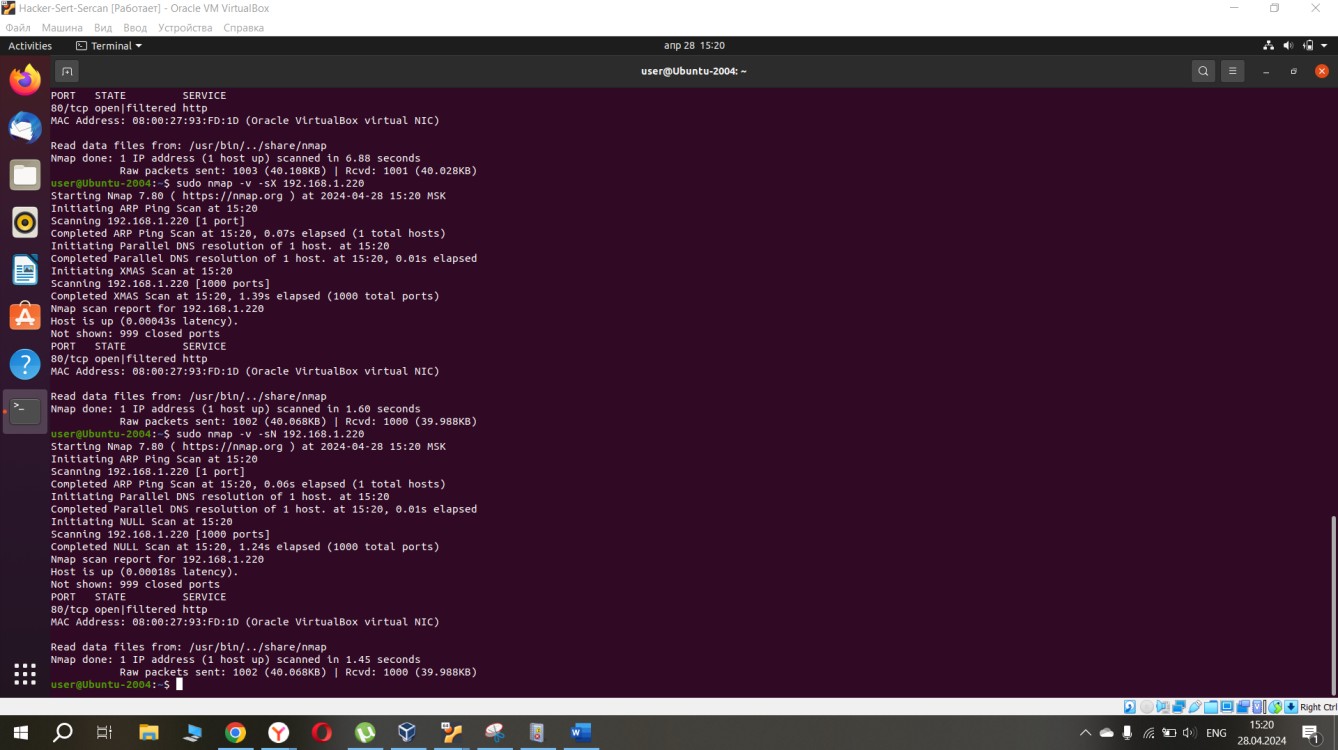
# Сканирования FIN, Xmas Tree и NULL

Тем не менее, межсетевой экран или другие защитные средства могут ожидать приходящие SYN-пакеты. Из-за этого зачастую такой метод сканирования не дает результата. Поэтому существует еще целая группа возможных способов сканирования, альтернативных TCP SYN. Это FIN, Xmas Tree и NULL-сканирования. Большинство операционных систем по умолчанию, согласно рекомендациям, должны ответить на такие пакеты, прибывшие на закрытые порты флагом RST. Важная деталь: ни одна операционная система семейства

Windows никогда не ответит RST пакетом на пришедший FIN, XmasTree или NULL пакет. Используя этот факт даже при подобных, в общем-то, не особо детальных сканированиях можно предположить, как минимум семейство операционных систем.

sudo nmap –sF 192.168.1.220 sudo nmap -sX 192.168.1.220 sudo nmap -sN 192.168.1.220

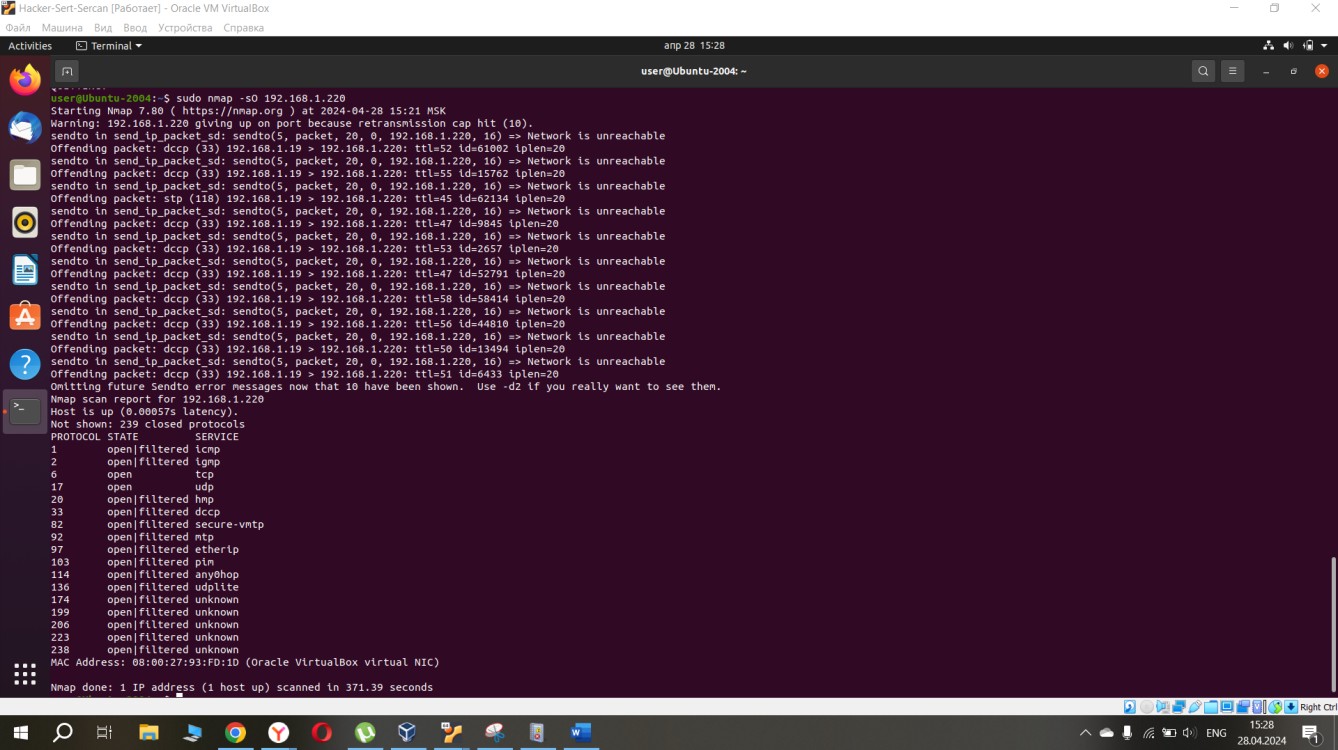




# Сканирование протоколов IP

Метод заключается в том, что хосту передаются IP пакеты без заголовков для каждого протокола сканируемого хоста. Если получено сообщение, говорящее о недоступности протокола, то этот протокол не поддерживается хостом. В противном случае — поддерживается.

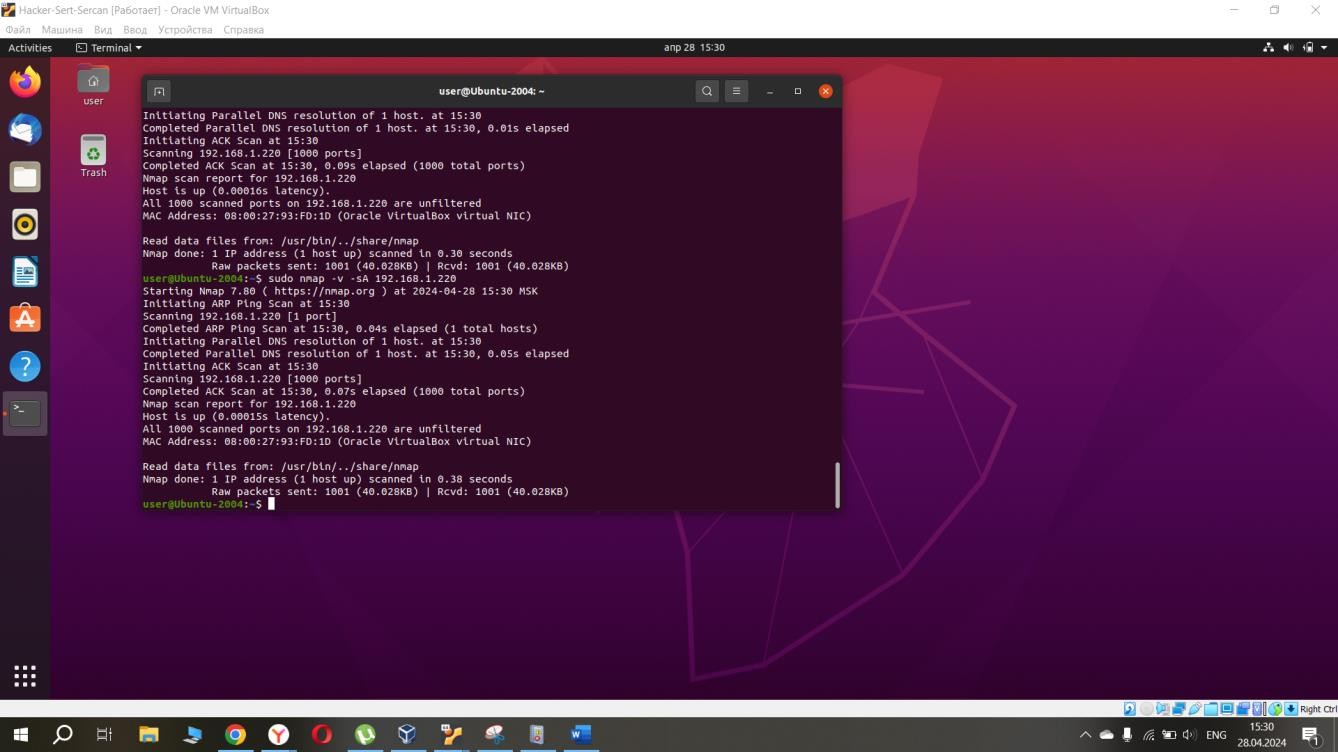
sudo nmap –sO 192.168.1.220



# ACK-сканирование

ACK сканирование заключается в передаче ACK пакетов на сканируемый порт. Если в ответ приходит RST пакет, порт классифицируется как не фильтруемый. Если нет ответа или пришел ответ в форме ICMP-сообщения о недоступности порта, порт считается

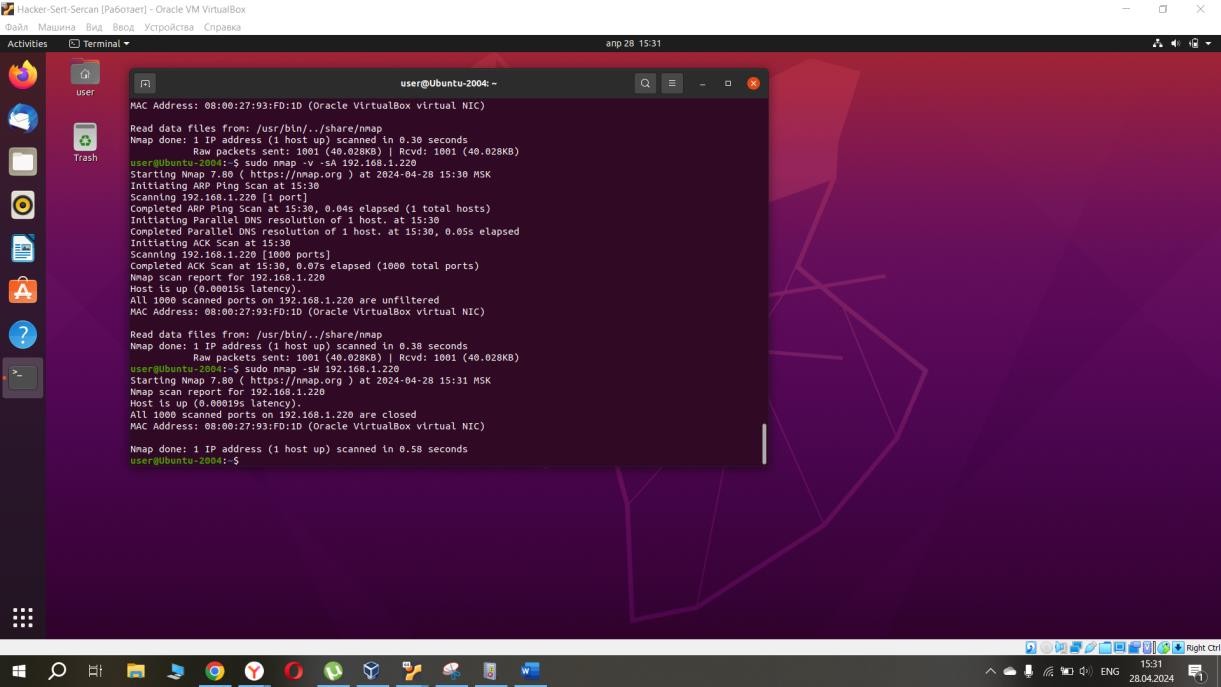
фильтруемым. Этот метод никогда не покажет состояние порта «открыт». sudo nmap –sA 192.168.1.220



# TCP Window

TCP Window — похоже на ACK сканирование, однако по значениям поля Initial Window TCP-пакета пришедшего в ответ, можно определить открытые порты.

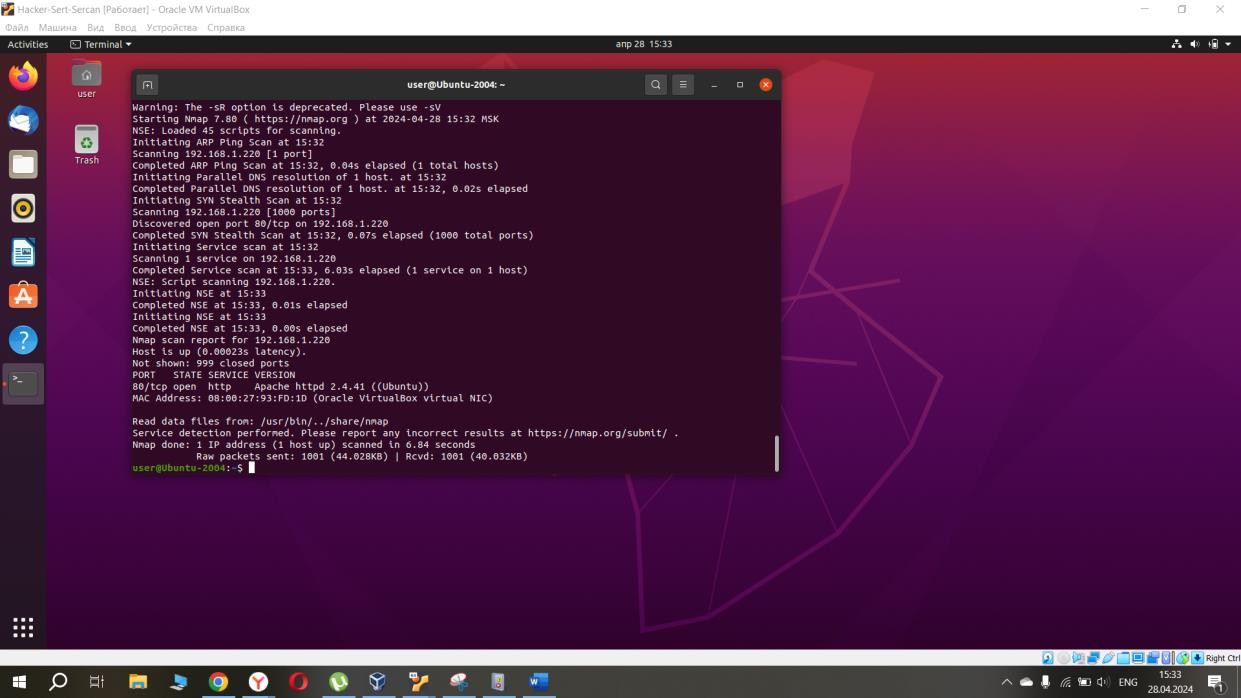
sudo nmap –sW 192.168.1.220



# RPC-сканирование

RPC-сканирование используется для определения программы, обслуживающей порт и её версии, и заключается в «затоплении» NULL- пакетами оболочки SunRPC открытых TCP или UDP портов хоста.

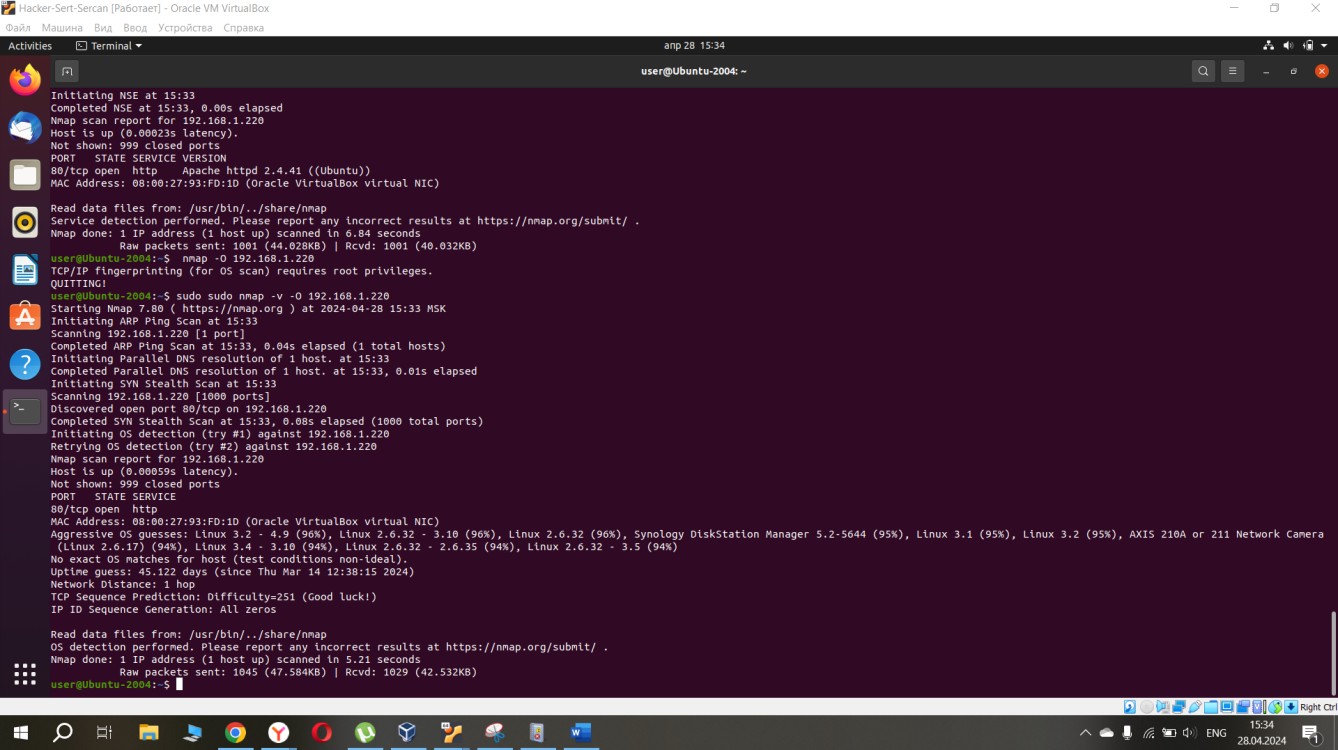
sudo nmap –sR 192.168.1.220



# Сканирование ОС

И, наконец, последнее — сканирование, используемое для определения ОС на сканируемом хосте.

sudo nmap –O 192.168.1.220

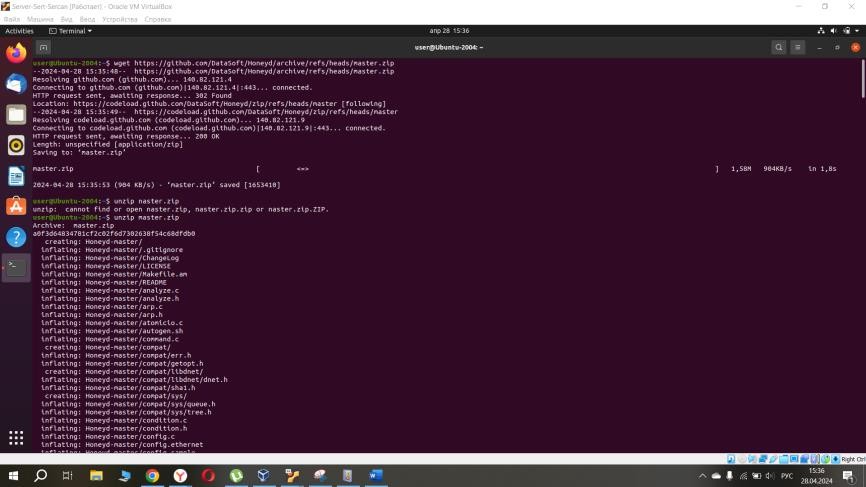


Следующим шагом переходим к установке и настройке Honeypot на Server.

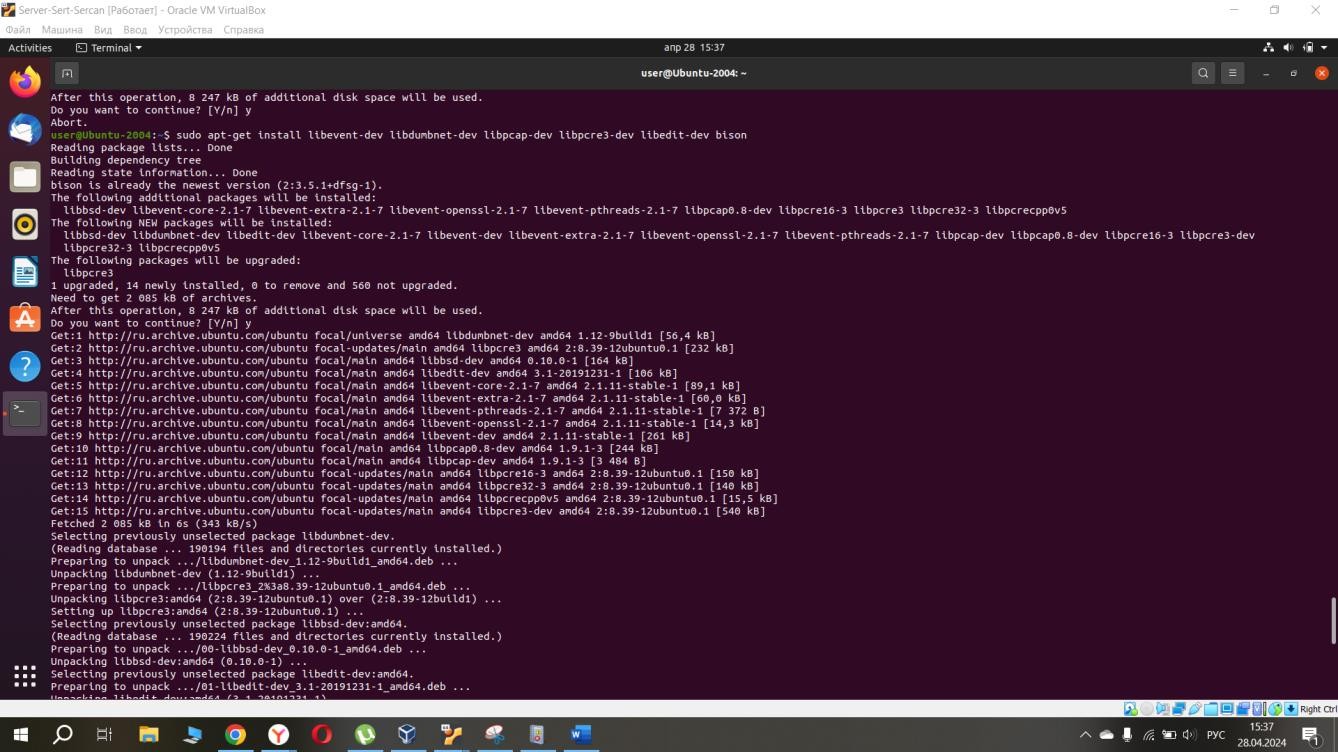
# Honeypot

Honeypot («Ловушка») - ресурс, представляющий собой приманку для злоумышленников. Фактически основная задача Honeypot — подвергнуться атаке или несанкционированному сканированию с целью изучения стратегии и методов сканирования и определения перечня средств, необходимых для предотвращения будущих атак. Суть работы Honeypot заключается в создании ловушек — образов систем, которые извне воспринимаются как полноценные машины с установленными на них операционными системами, а,

следовательно, поддающиеся сканированию.

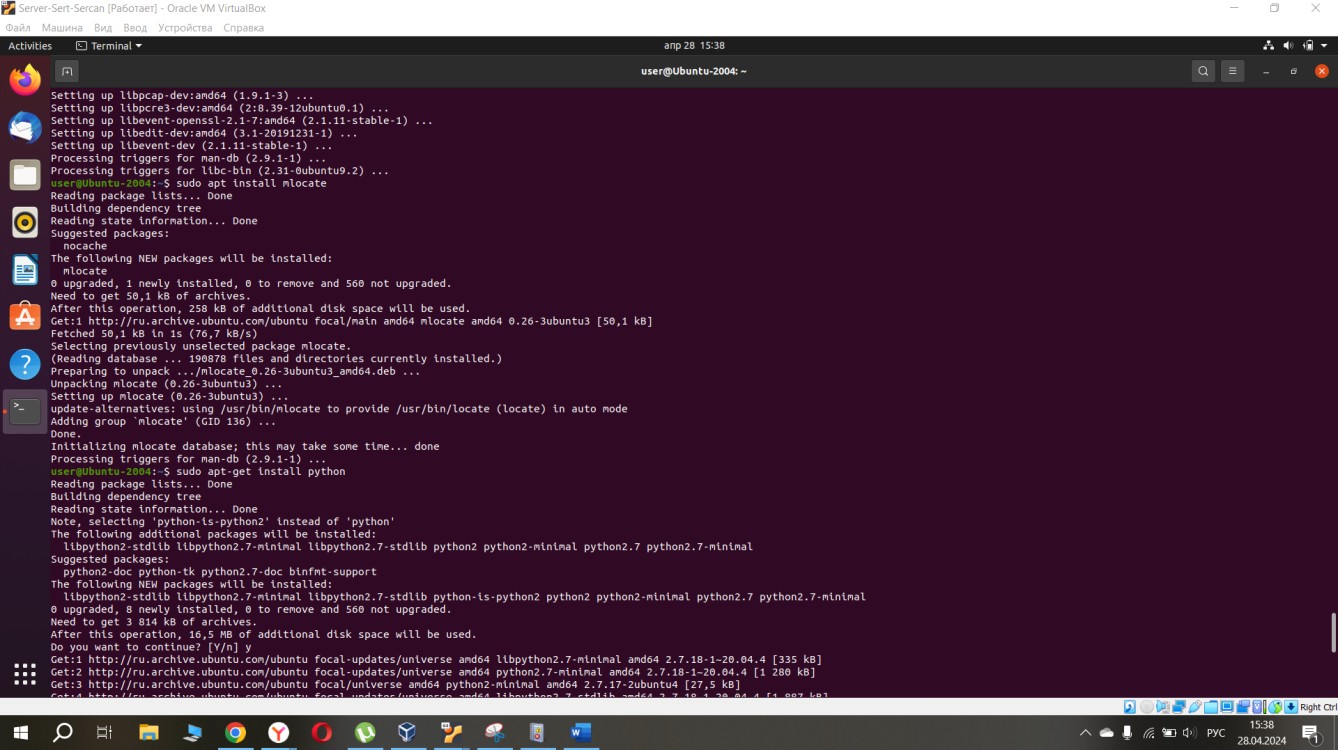


Скачали и разархивировали файл Honeypot. Скачиваем и устанавливаем недостающие пакеты.

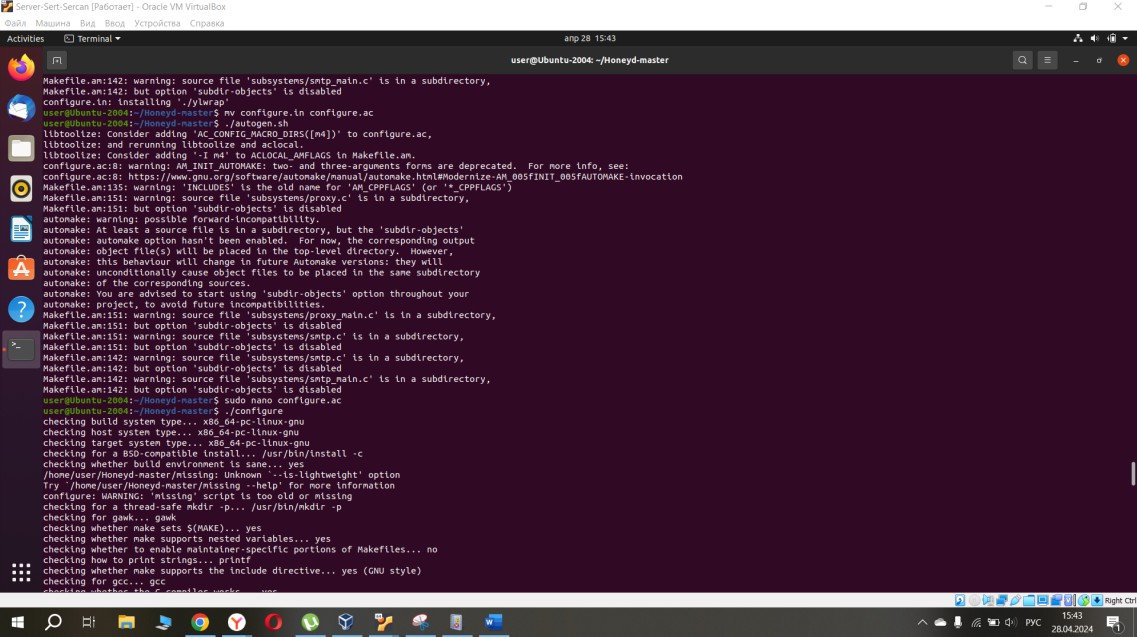


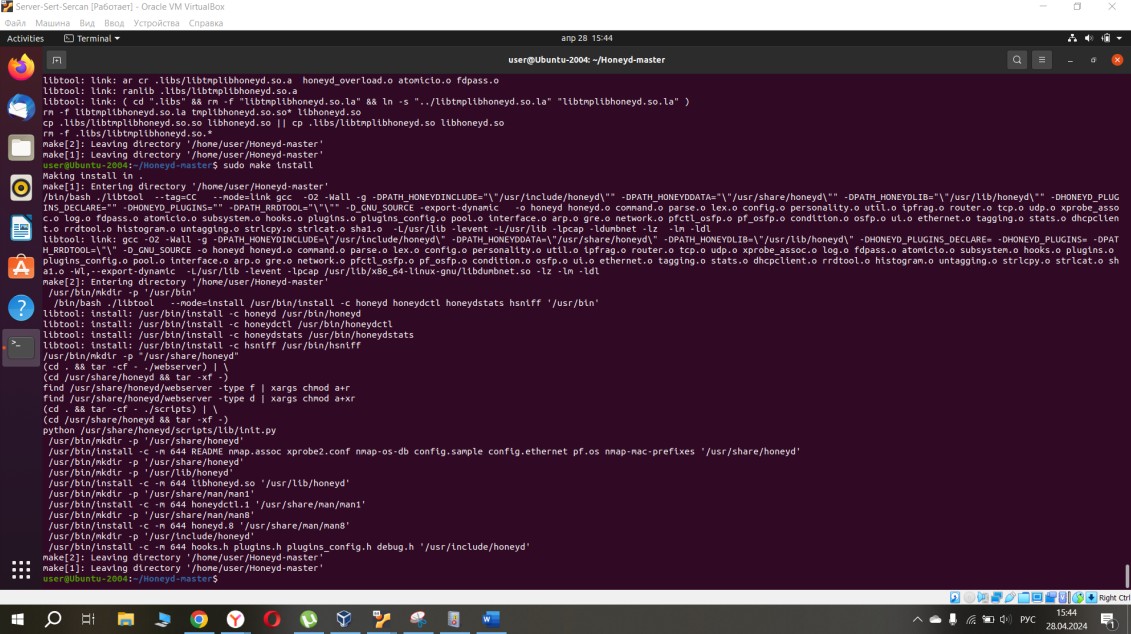
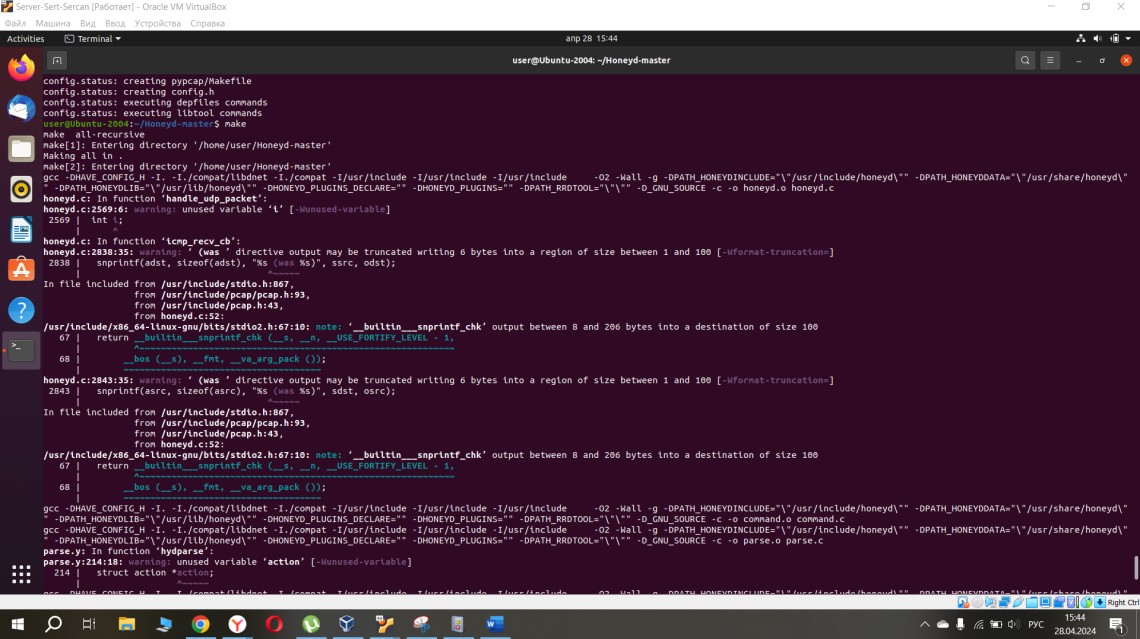
Переходим к настройке и сборке.

Скачаем mlocate и интерпритатор python, чтобы успешно провести сборку и установку.



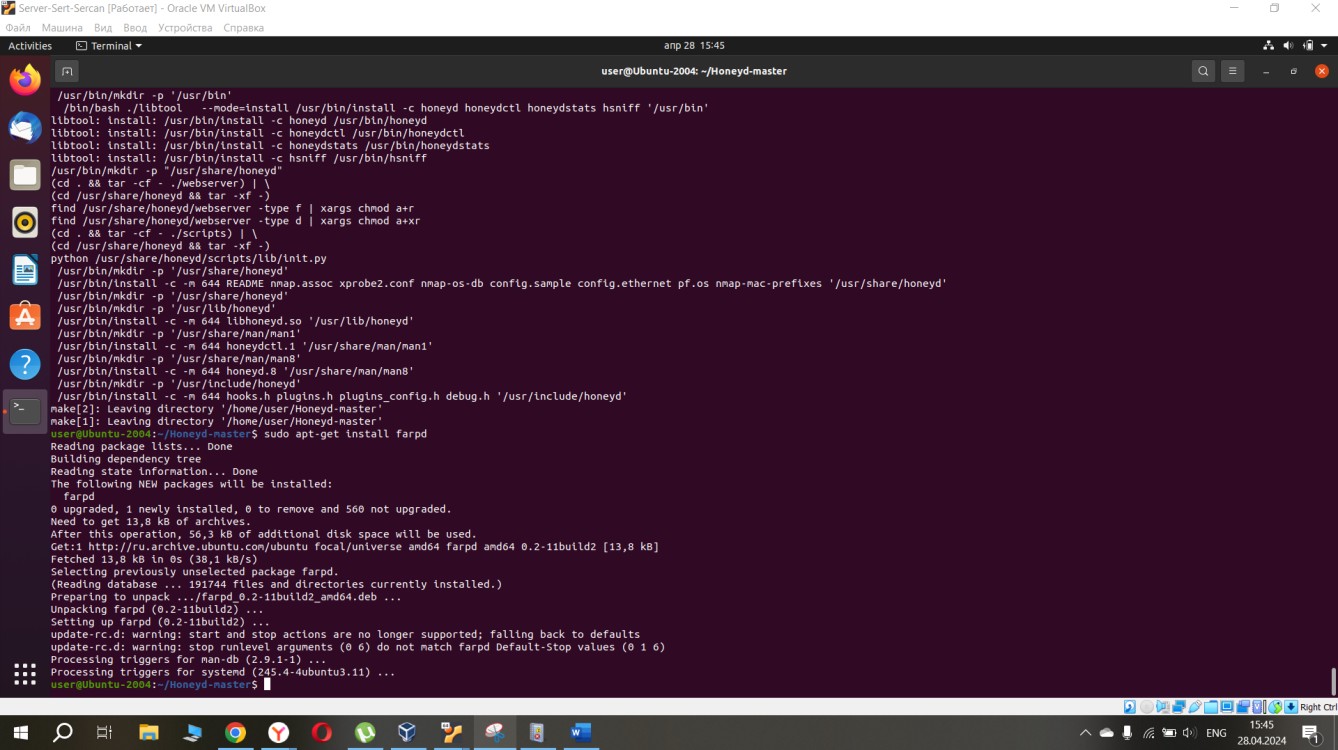
Выполним последовательно команды: ./autogen.sh, ./configure, make, sudo make install, перейдя в нужный каталог.



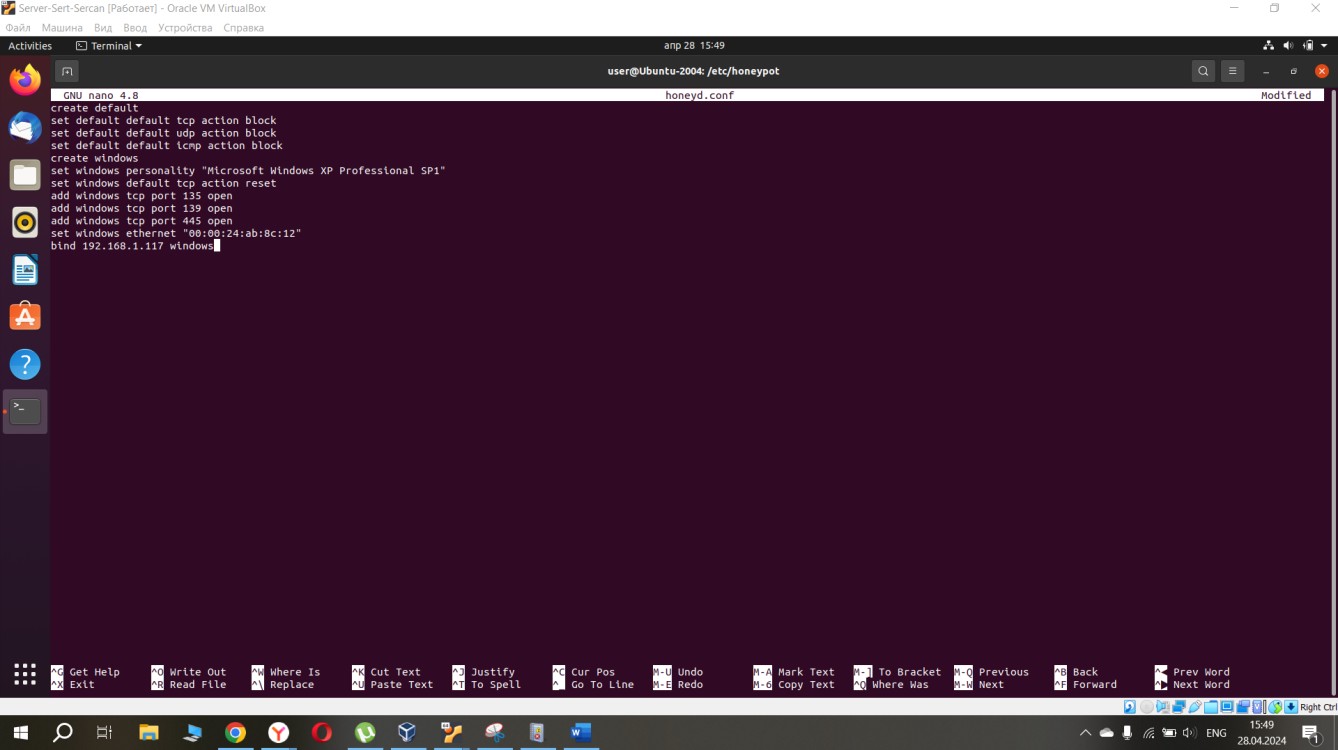


Все успешно сделано.

Установим farpd.

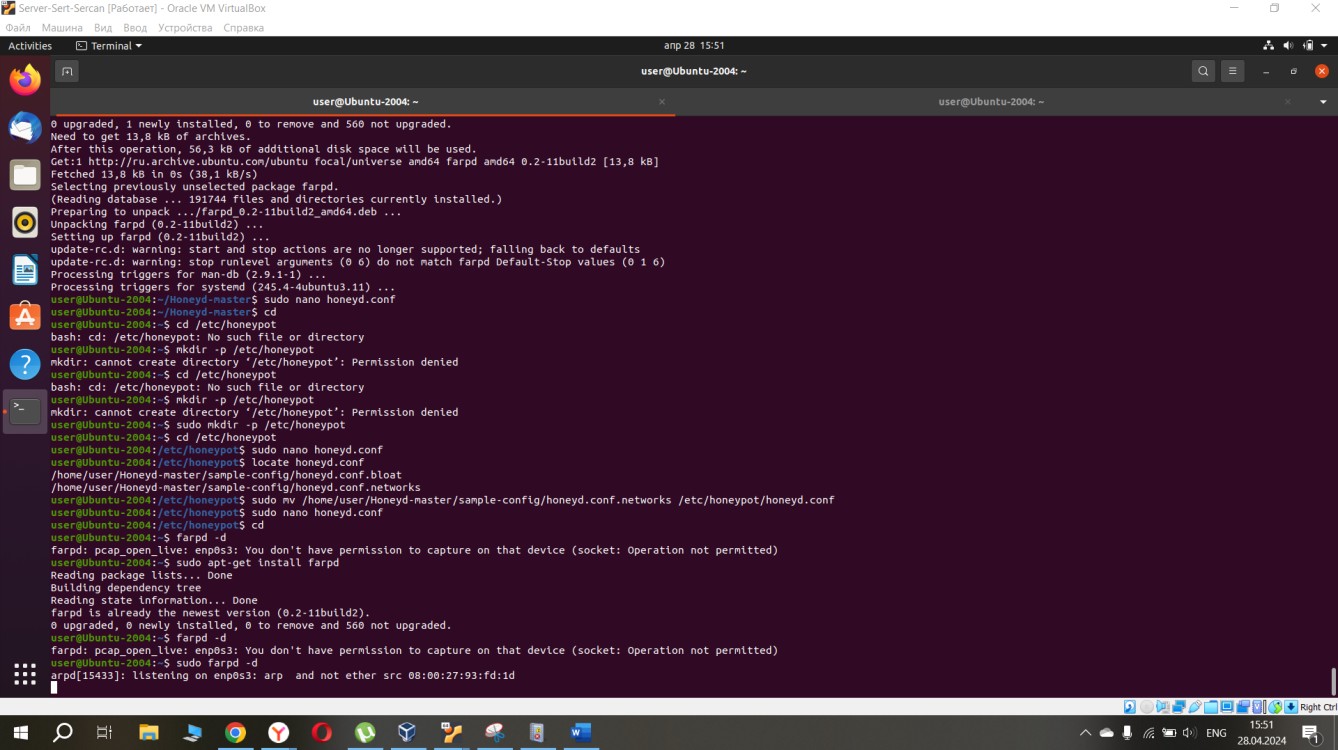


Сделаем нашу конфигурацию в honeyd.conf

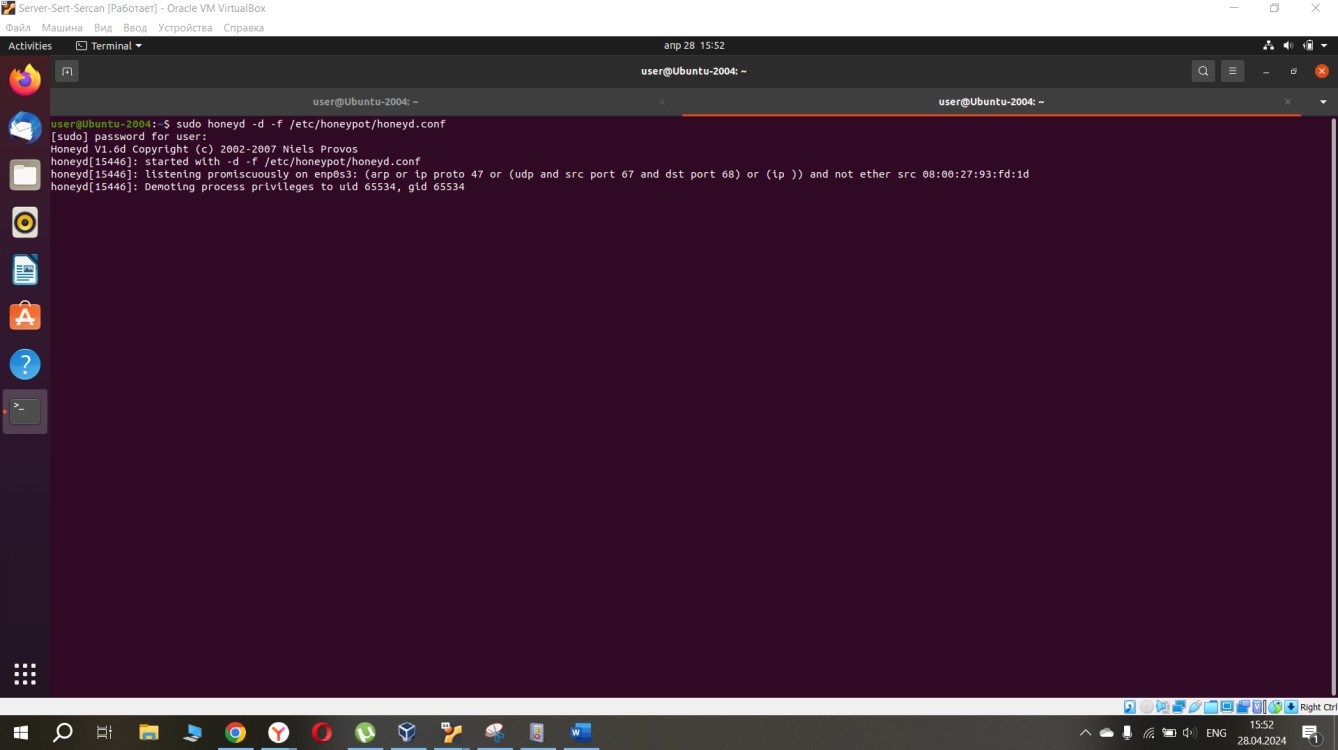


Сохраним и запустим honeypot.

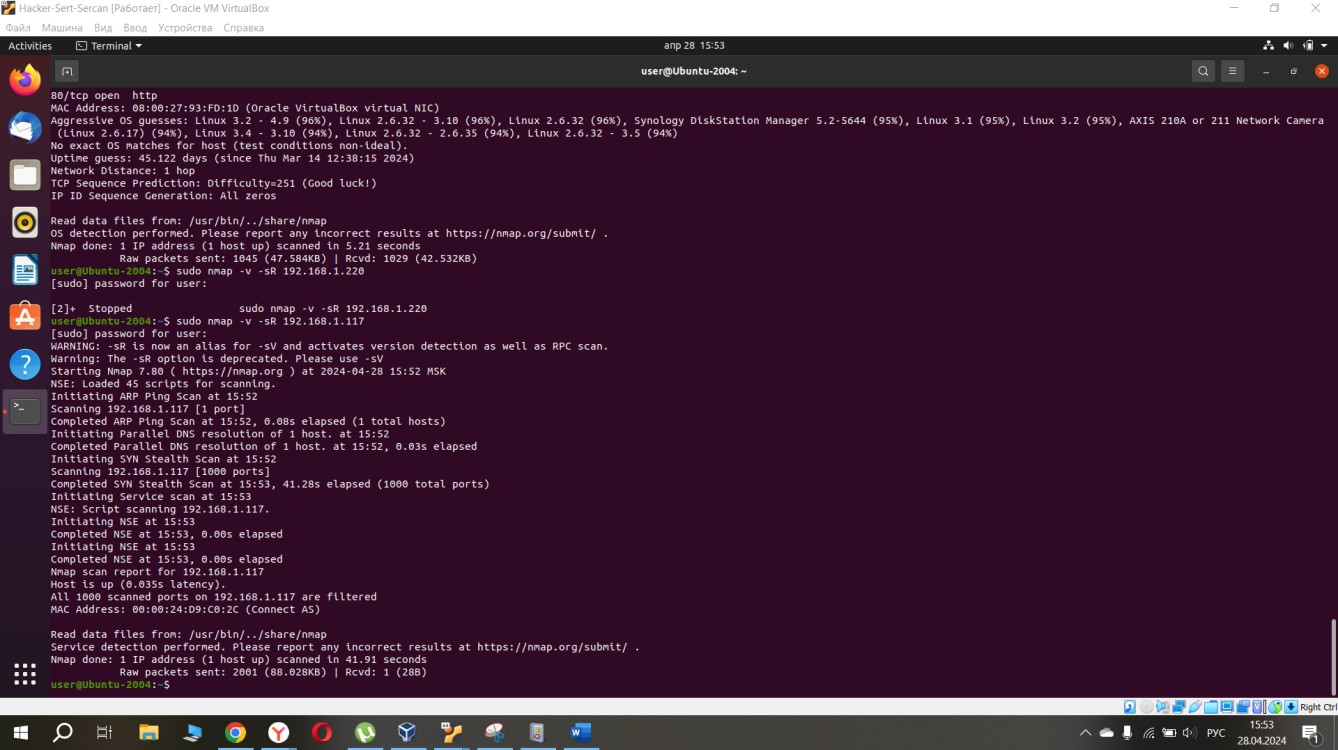
Запуск fardp:

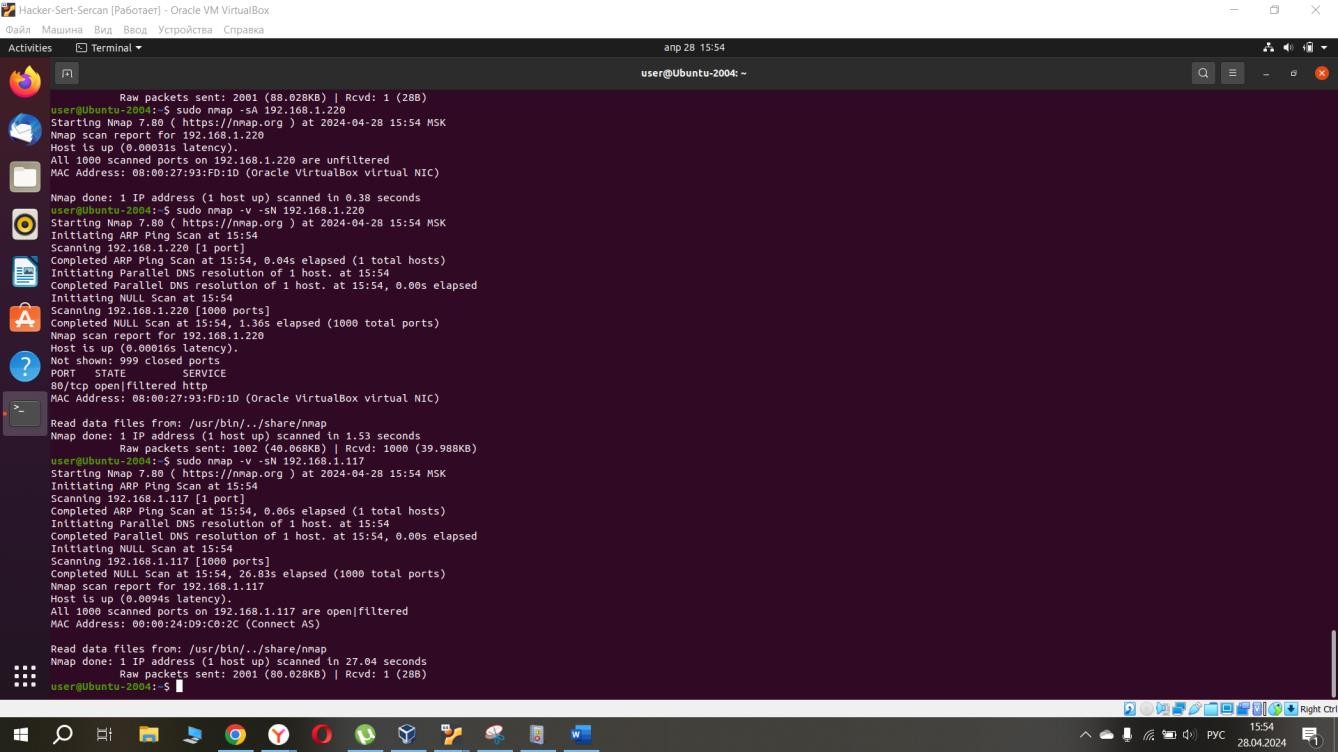


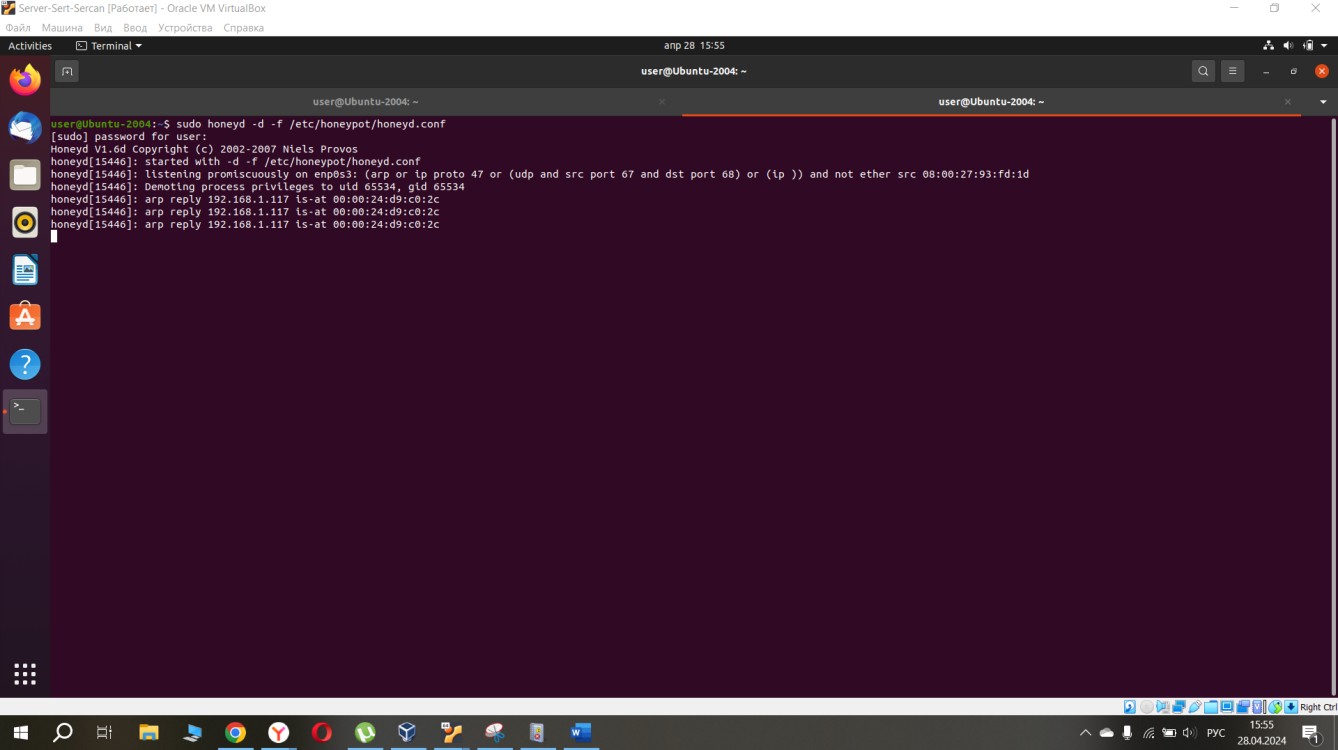
Запуск honeypot:

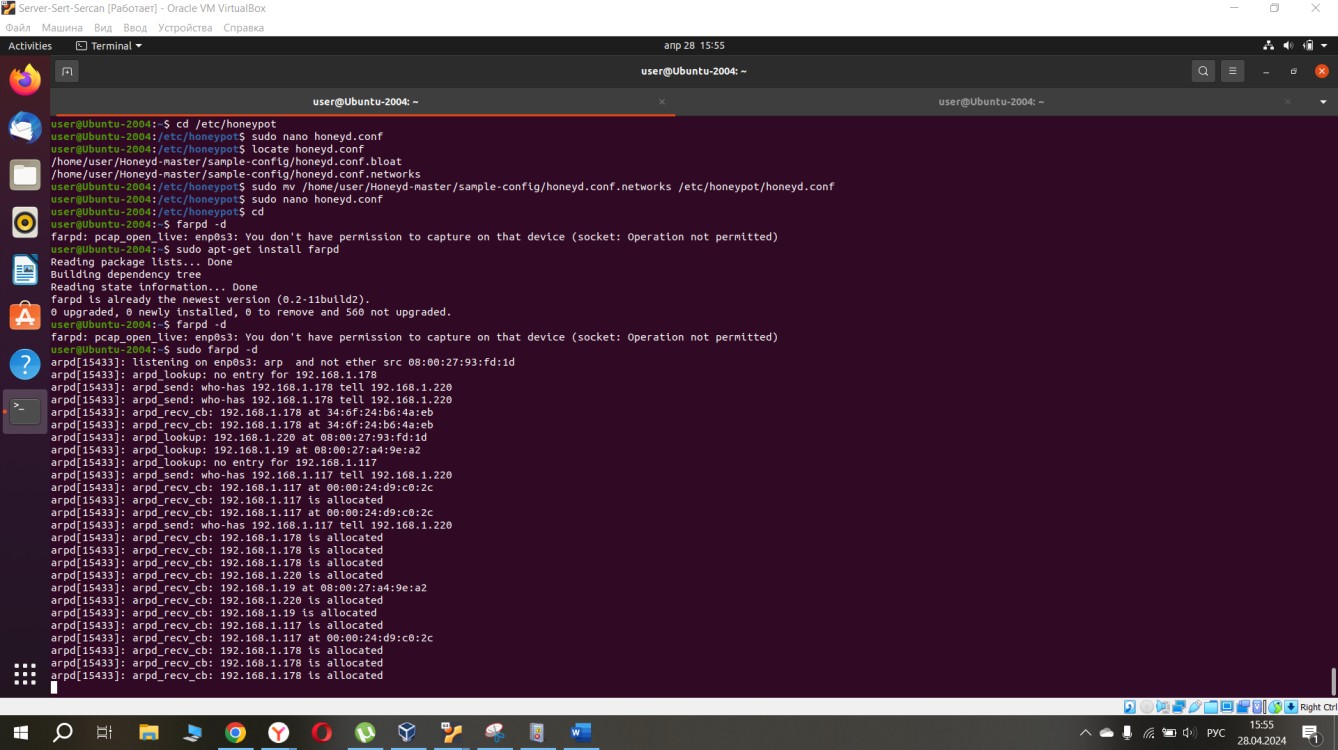


Делаем сканирования с Hacker и смотрим на реакции.









Все успешно выполнено.

Вывод: В ходе выполнения лабораторной работы мы провели исследование безопасности сети с использованием Honeypot и Nmap.

Nmap был использован для сканирования сети с целью обнаружения активных узлов и открытых портов. С помощью Nmap мы смогли получить информацию о конфигурации сети, активных службах и потенциальных уязвимостях, которые могут быть использованы злоумышленниками для атак.

Honeypot был развернут в сети в качестве приманки для злоумышленников. Мы наблюдали активность на Honeypot, включая попытки сканирования портов, атаки и другие вредоносные действия. Это позволило нам лучше понять характер угроз и методы атак, используемые в сети.

Вопросы к лабораторной работе

1. Что такое статический и динамический IP-адреса? В чём разница?

IP-адрес называют **статическим** (постоянным, неизменяемым), если он назначается пользователем в настройках устройства, либо если назначается автоматически при подключении устройства к сети и не может быть присвоен другому устройству.

IP-адрес называют **динамическим** (непостоянным, изменяемым), если он назначается автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, указанного в сервисе назначавшего IP-адрес (DHCP).

1. В чём заключается метод сканирование протоколов IP?

Метод заключается в том, что хосту передаются IP пакеты без заголовков для каждого протокола сканируемого хоста. Если получено сообщение о недоступности протокола, то этот протокол не поддерживается хостом. В противном случае – поддерживается.

1. На какие пакеты большинство ОС должны ответить флагом RST?

TCP-SYN На пакеты с установленным флагом SYN, которые направлены на закрытые или несуществующие порты.

1. Назначение, цели, описание Honeypot.

Honeypot — подвергнуться атаке или несанкционированному сканированию с целью изучения стратегии и методов сканирования и определения перечня средств, необходимых для предотвращения будущих атак. Суть работы Honeypot заключается в создании ловушек — образов систем, которые извне воспринимаются как полноценные машины с установленными на них операционными системами, а, следовательно, поддающиеся сканированию.

1. Какие цели может преследовать злоумышленник, взламывая сервера?

**Установка вредоносного ПО ,** **Получение контроля**, **Нарушение работы,** **Финансовая выгода**

6. Какое наказание предусмотрено в РФ за взлом?

В РФ за взлом предусмотрено наказание по статье 272 УК РФ, включающее штраф, обязательные или исправительные работы, арест или лишение свободы на срок до 7 лет в зависимости от тяжести преступления.

7. Как выявлять Honeypot?

**Аномалии в поведении**: Проверка необычных сетевых ответов или задержек.

**Проверка IP-адресов**: Сравнение IP-адреса с известными базами данных Honeypot.

**Активность портов**: Подозрительная активность на неиспользуемых или редко используемых портах.

**Изучение баннеров**: Анализ информации, возвращаемой баннерами, на соответствие реальным системам.

**Ловушки и маркеры**: Определение использования известных Honeypot-технологий или ловушек.

8. Что такое DHCP?

сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

9. Для чего используется RPC-сканирование?

RPC-сканирование используется для определения программы, обслуживающей порт и её версии, и заключается в «затоплении» NULL- пакетами оболочки SunRPC открытых TCP или UDP портов хоста.

10. Перечислите основные методы сканирования Nmap.

* SYN Scan (sS):
* TCP Connect Scan (sT):
* UDP Scan (sU):
* Xmas Scan (sX):
* FIN Scan (sF):
* NULL Scan (sN):
* ACK Scan (sA):
* Window Scan (sW):
* Maimon Scan (sM):
* Idle Scan (sI):