**Министерство науки и высшего образования Российской Федерации**

федеральное государственное автономное образовательное учреждение высшего образования

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Отчет**

по лабораторной работе №6

по дисциплине «**Телекоммуникационные системы и технологии**»

Авторы: Юрпалов С. Н.,

Кошкин М.С.

Факультет: ИТиП

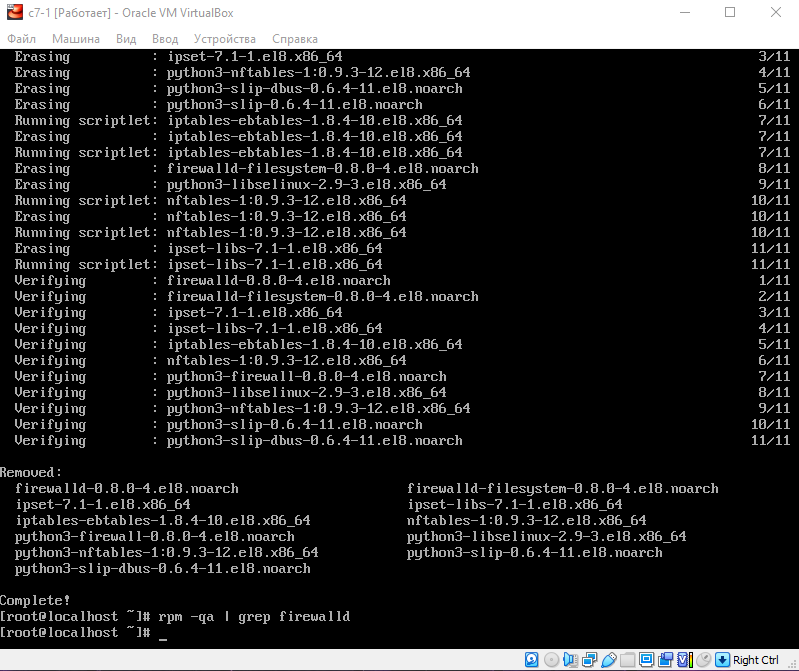
Группа: М33051

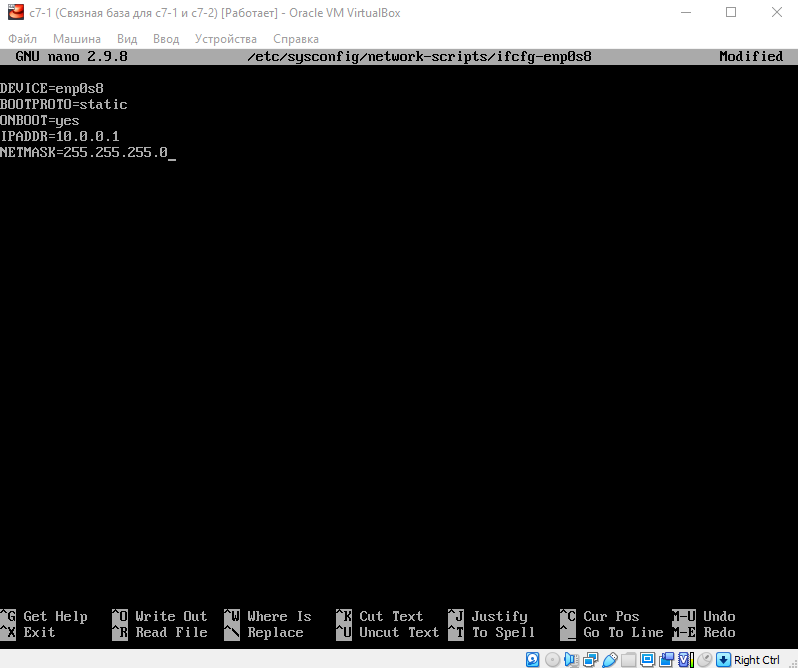


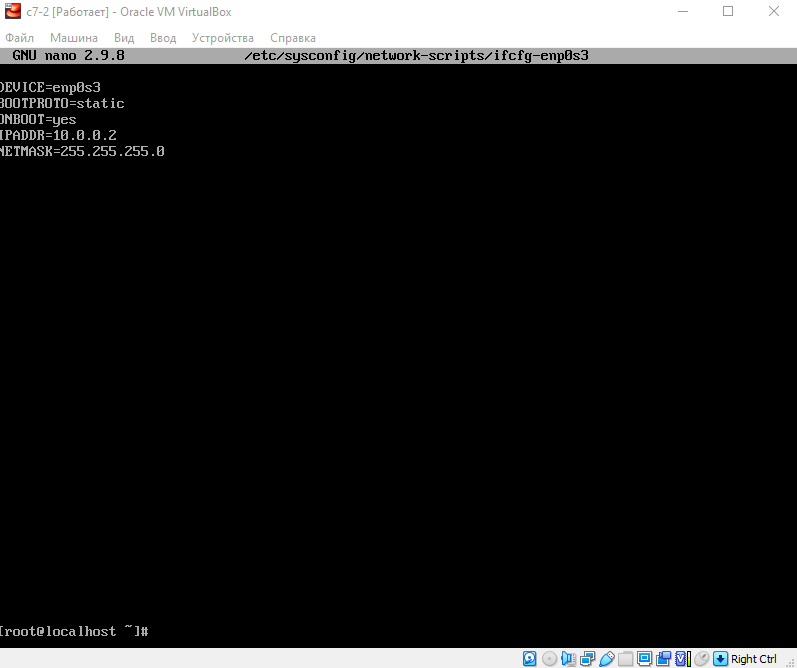
Санкт-Петербург 2023

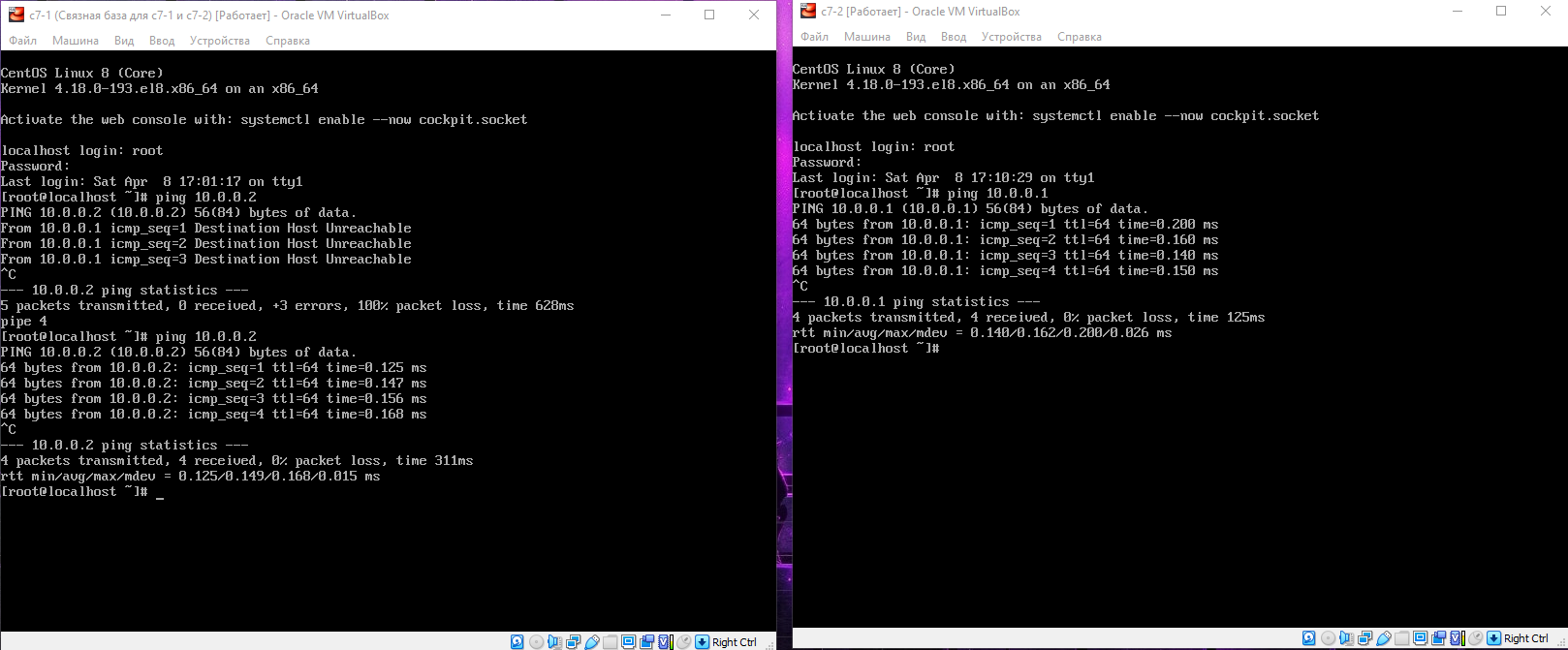
Ход работы

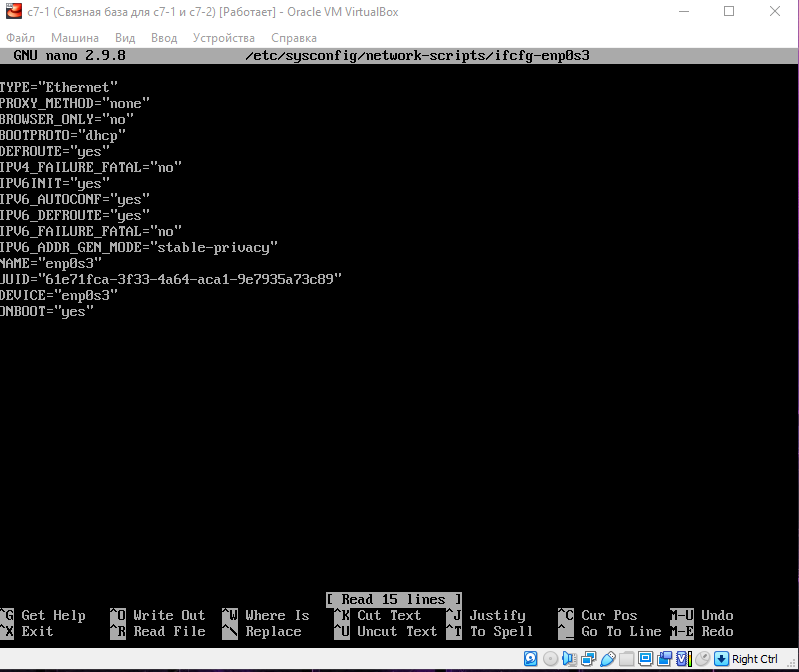
**Часть 1:**

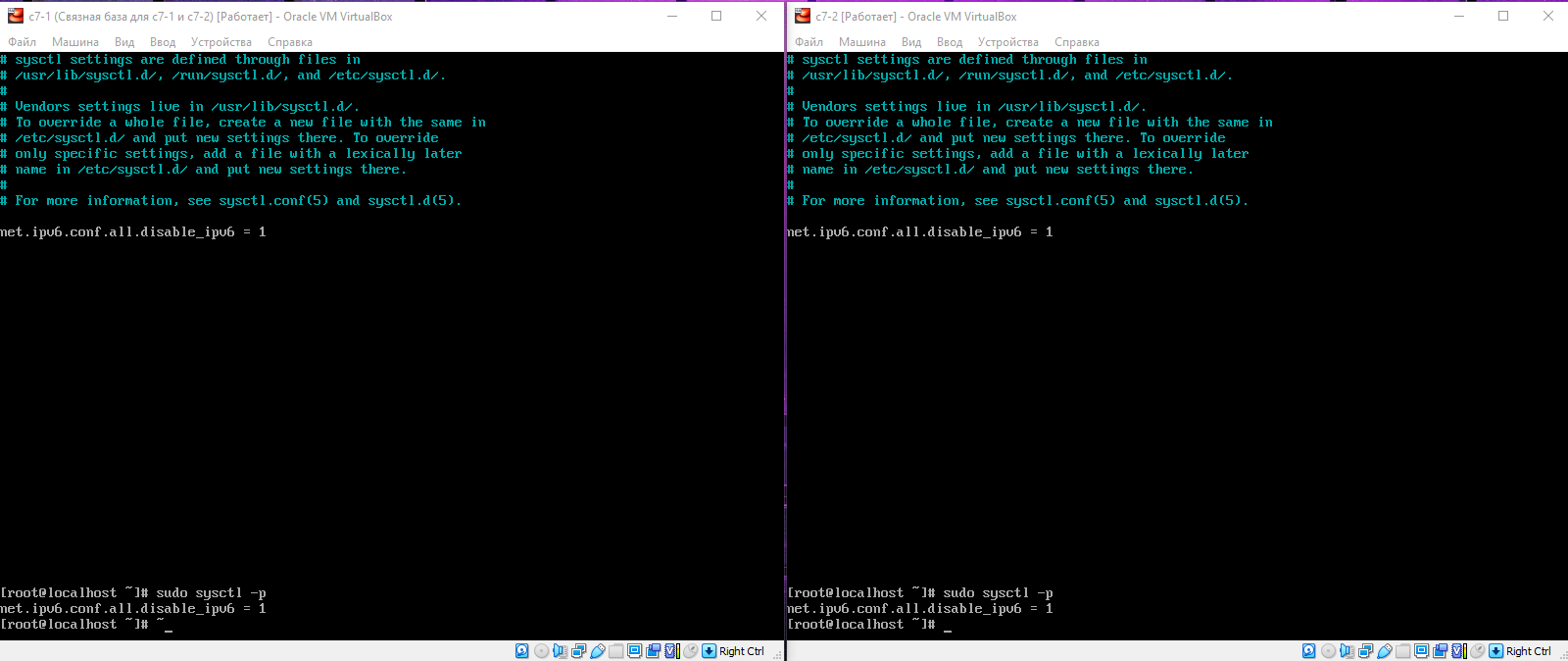


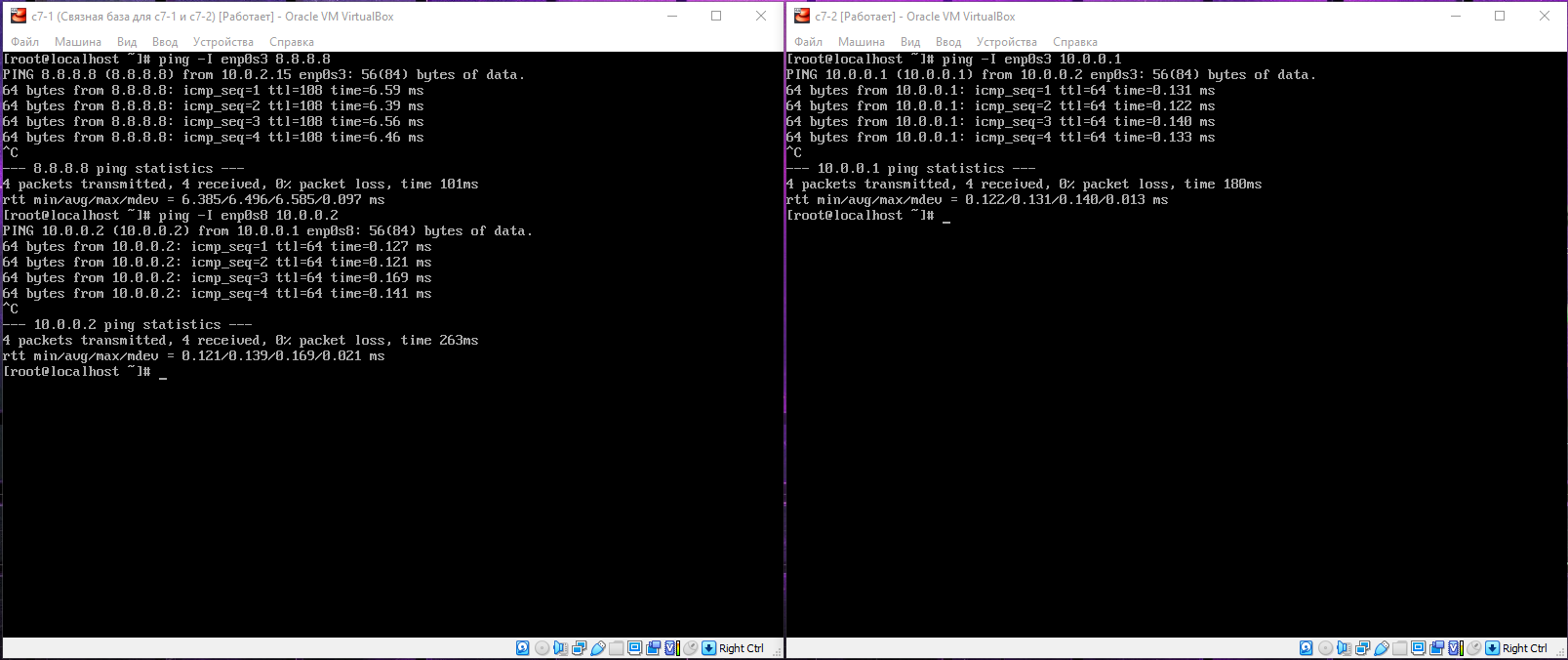












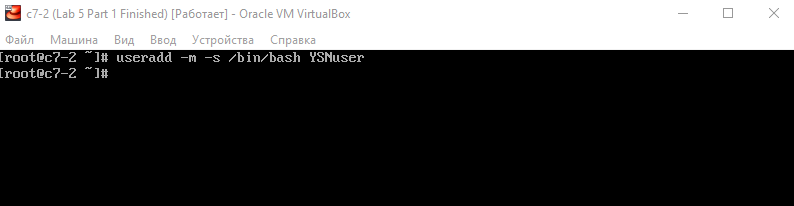


/etc/sysctl.conf

net.ipv4.ip\_forward = 1

**Часть 2:**

sudo passwd YSNuser 12345



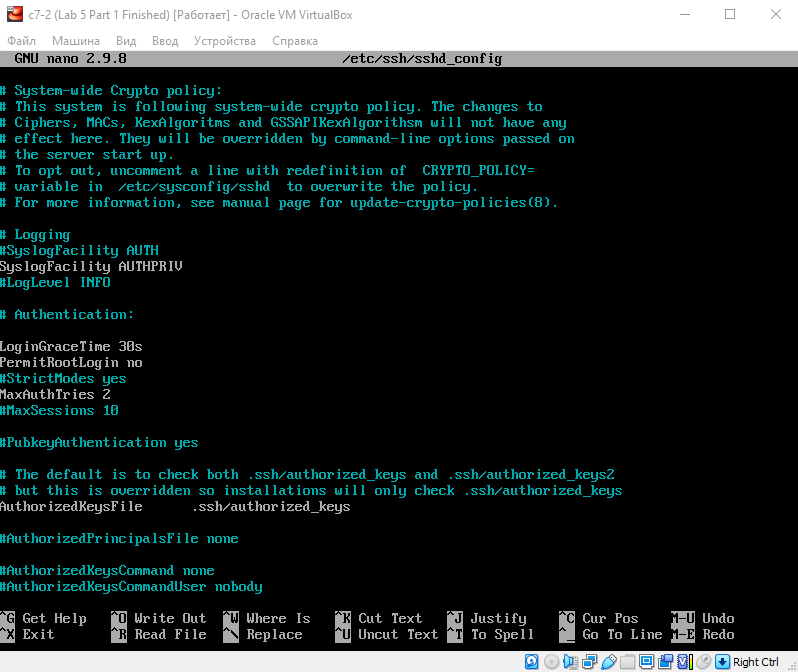
/etc/ssh/sshd\_config

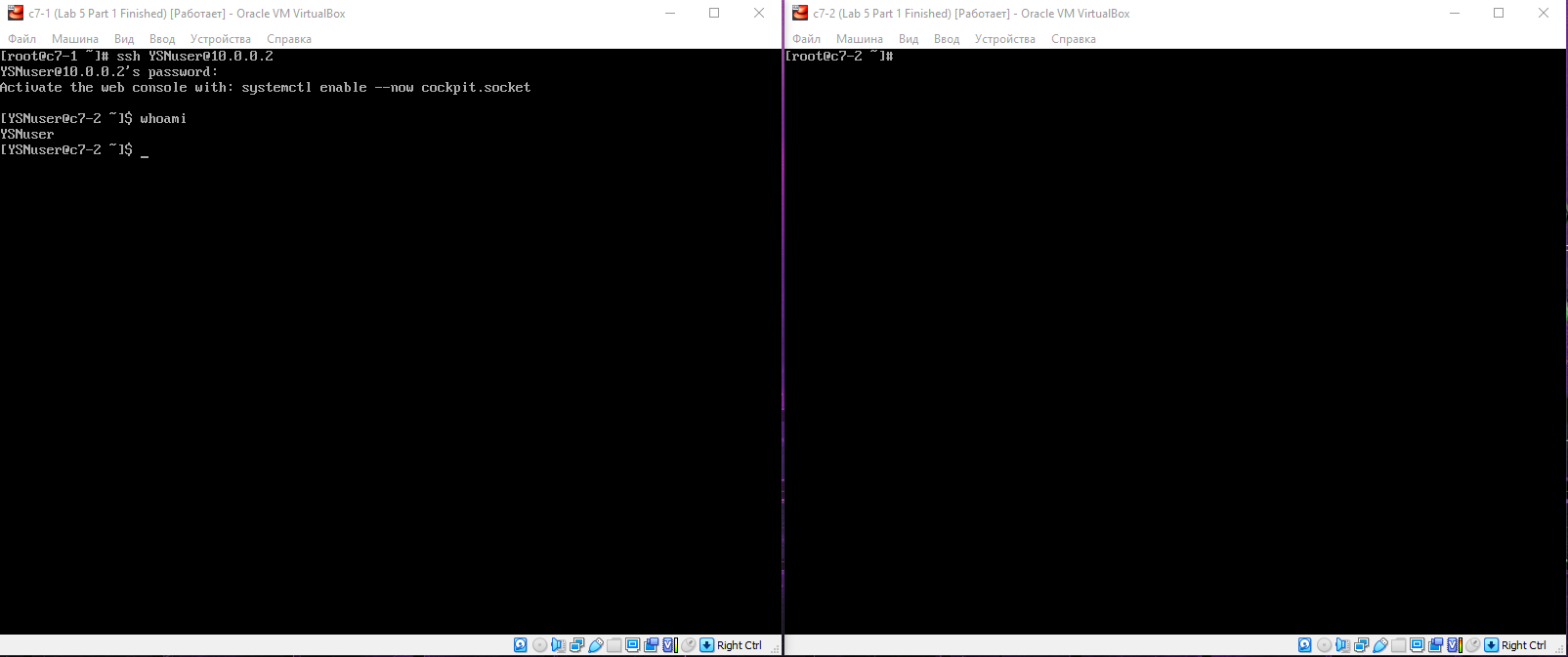
PermitRootLogin no

MaxAuthTries 2

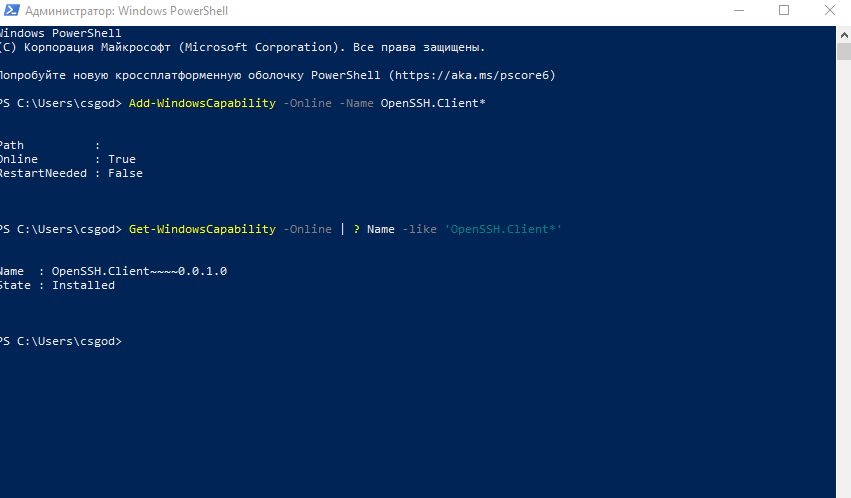
LoginGraceTime 30s

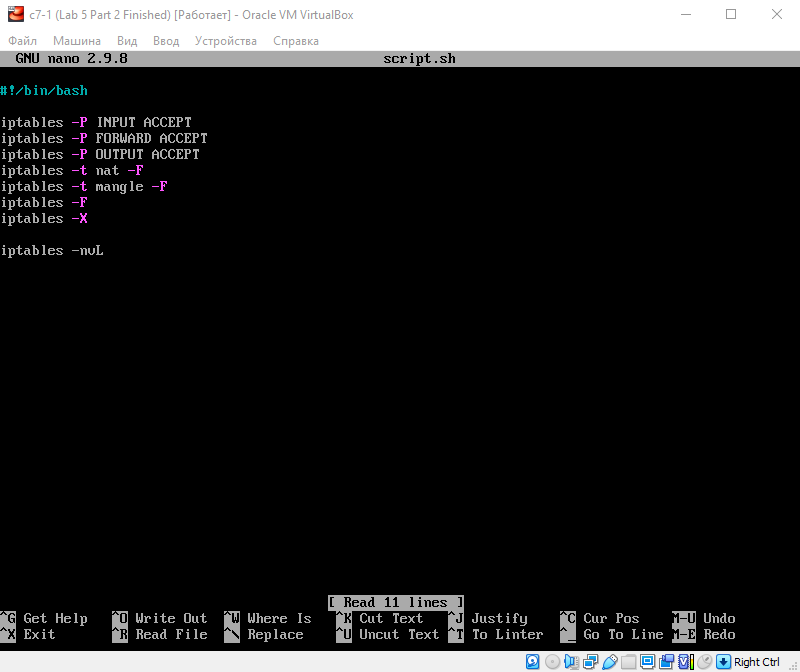
UseDNS no

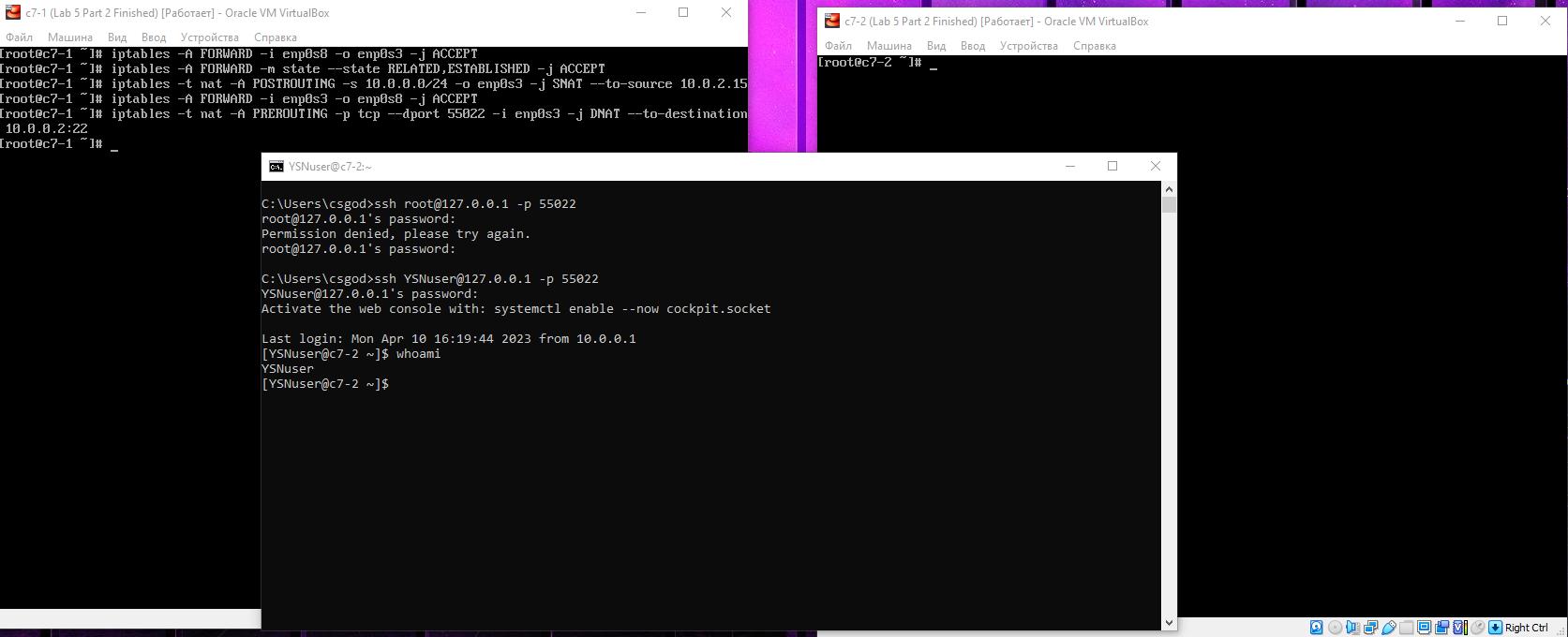




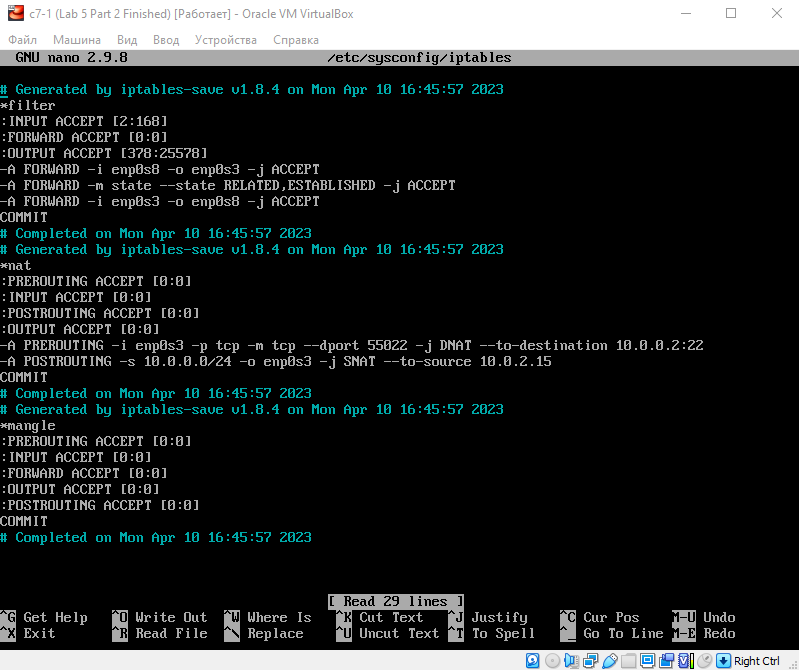
**Часть 3:**

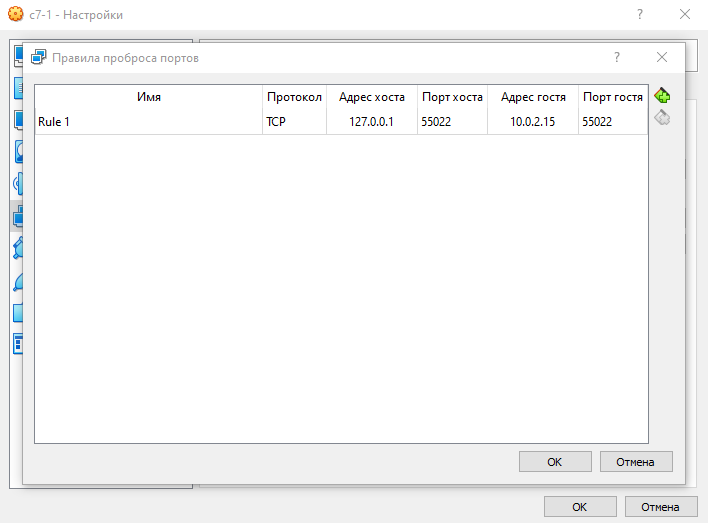


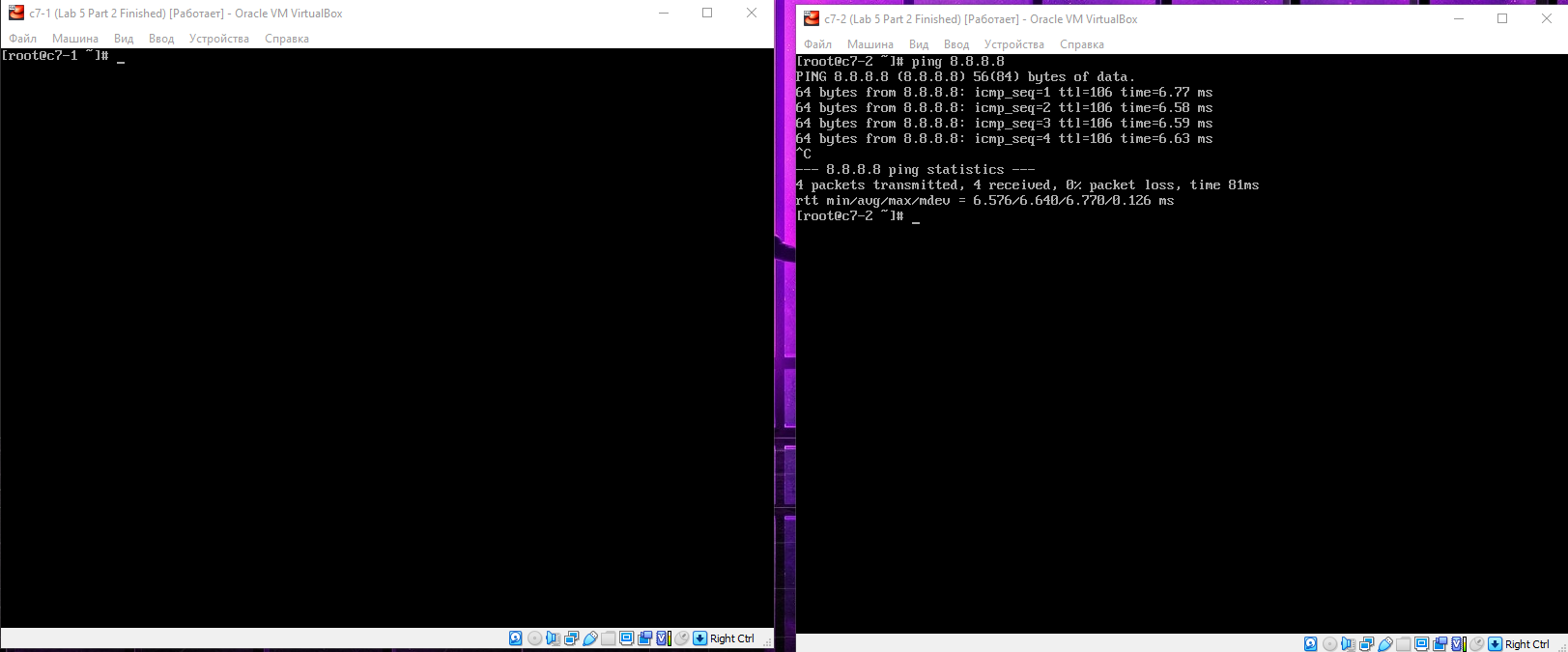




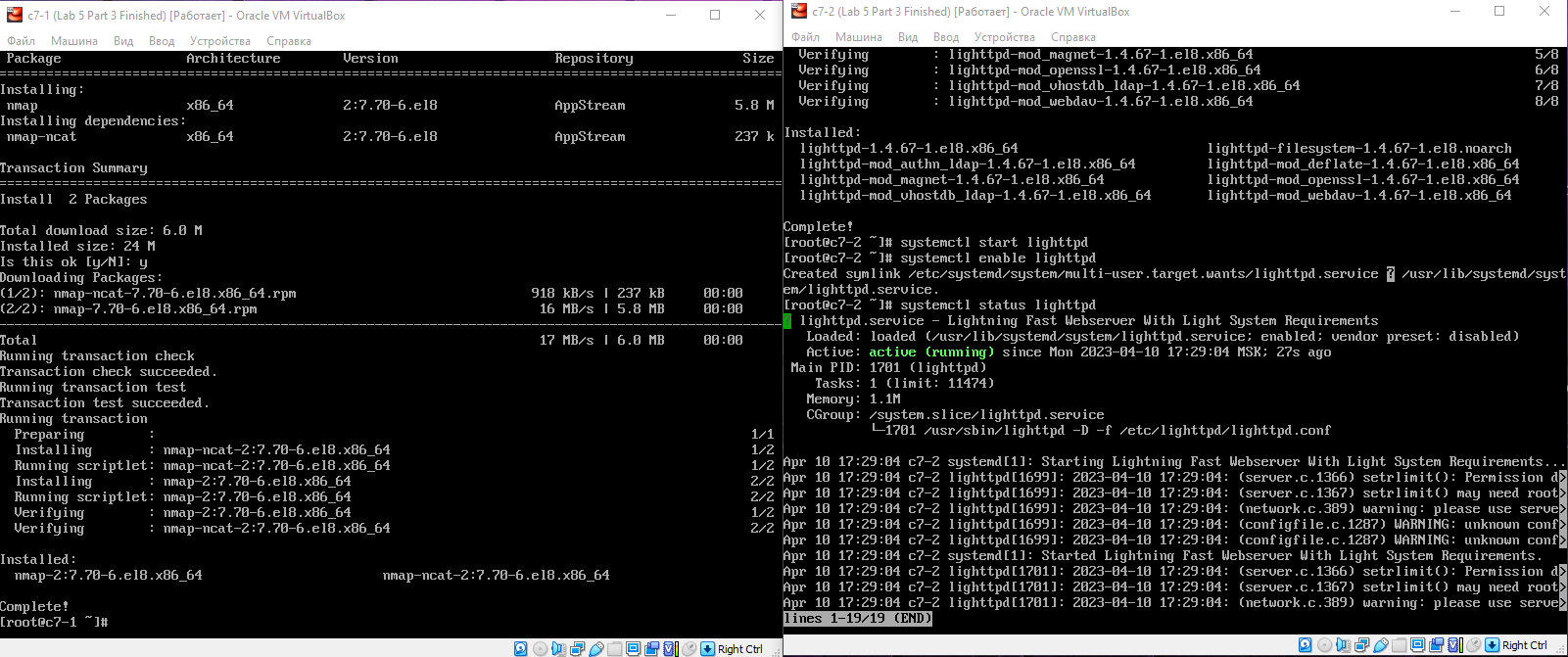
sudo iptables-save > /etc/sysconfig/iptables

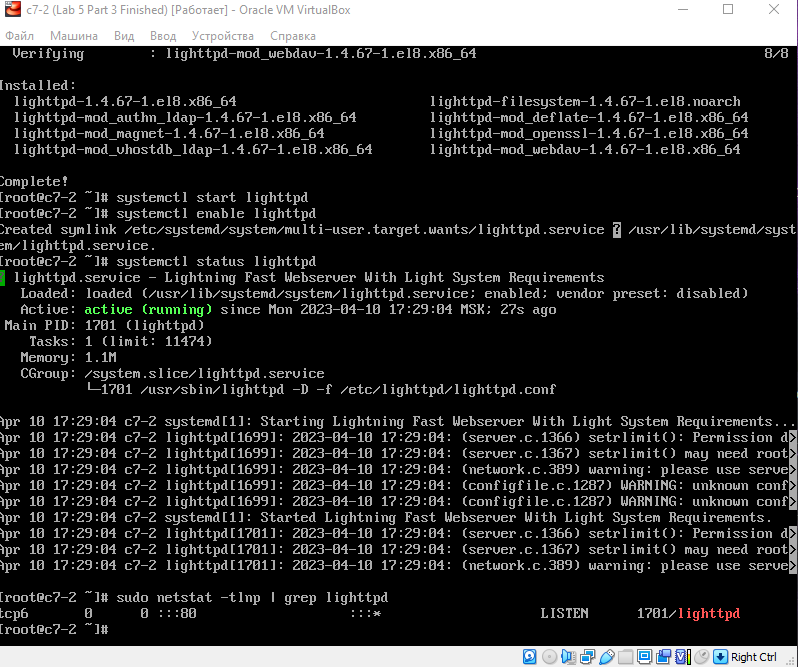


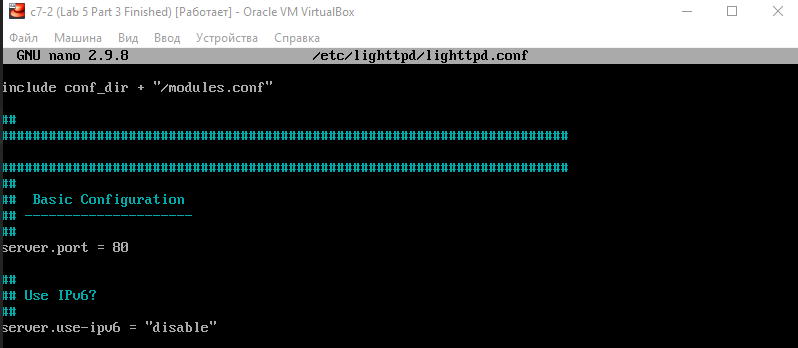


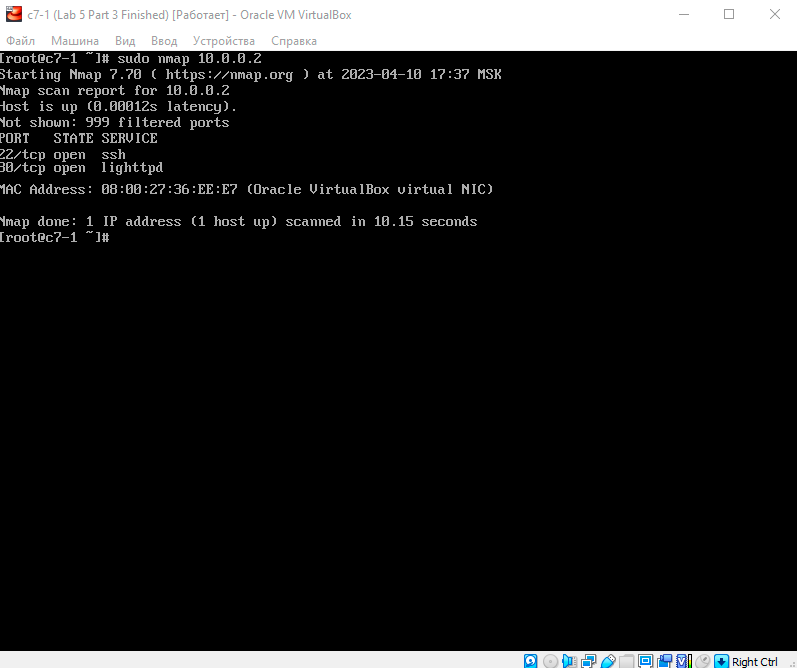


**Часть 4:**

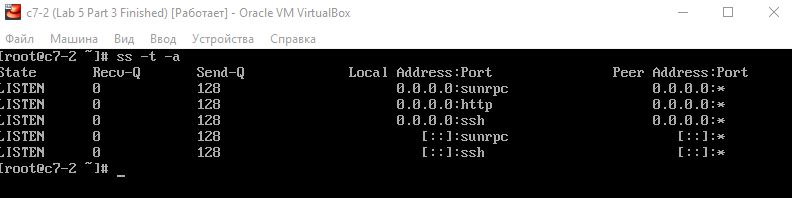


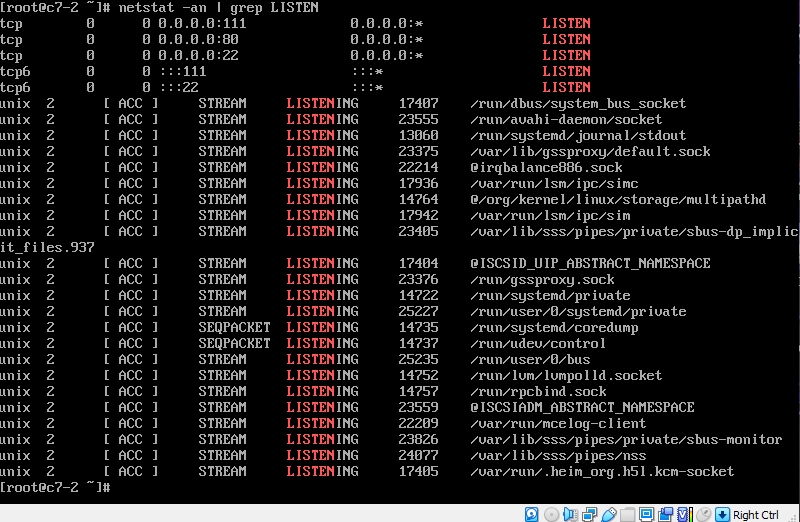


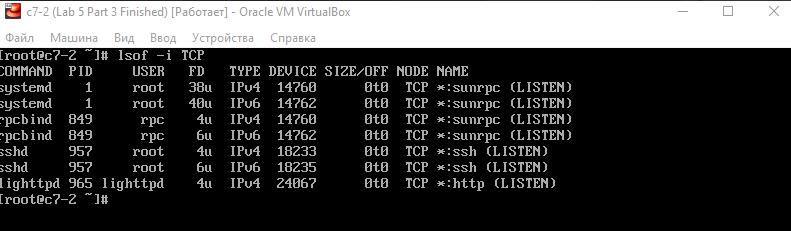


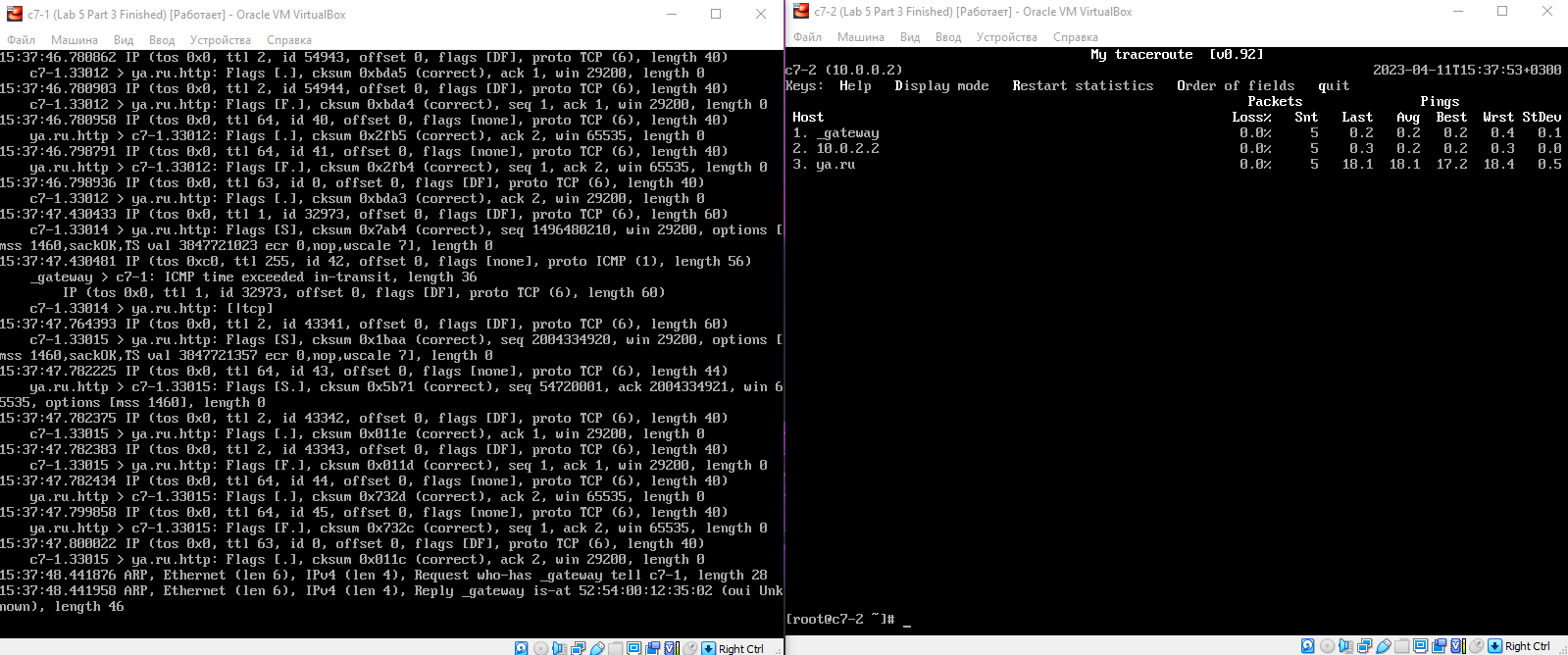


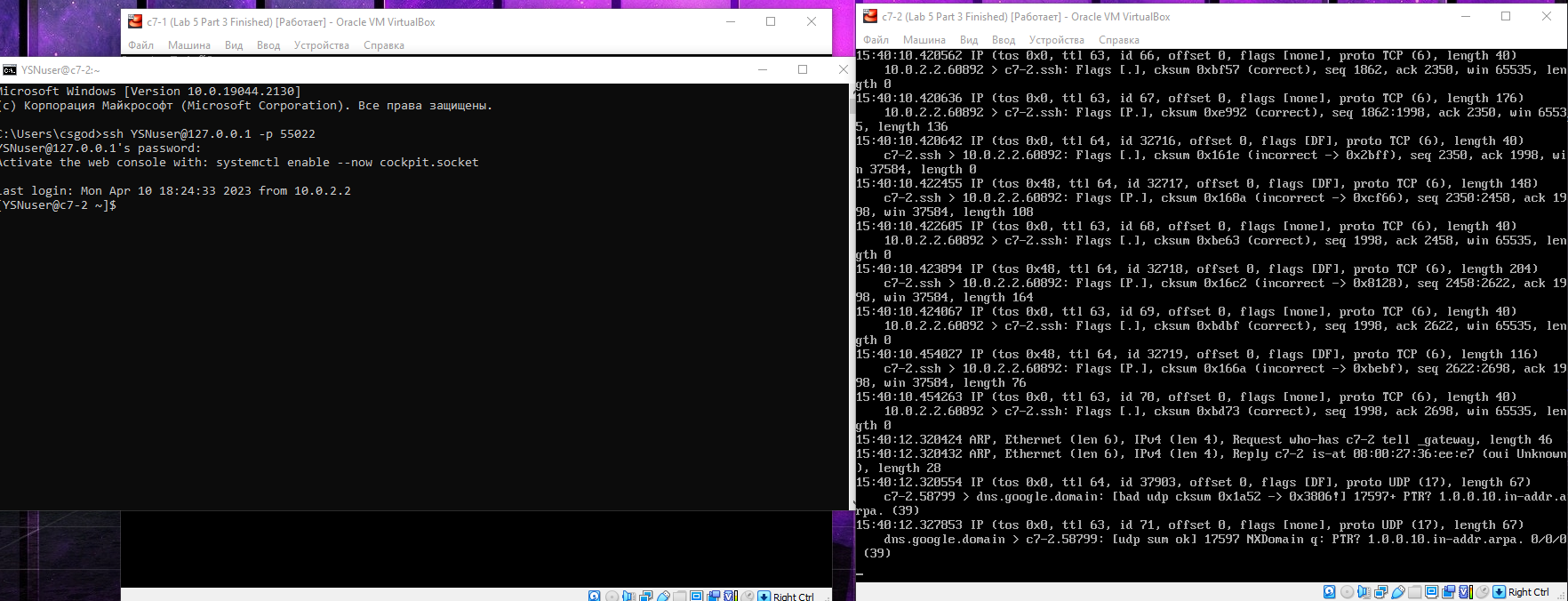
**Часть 5:**

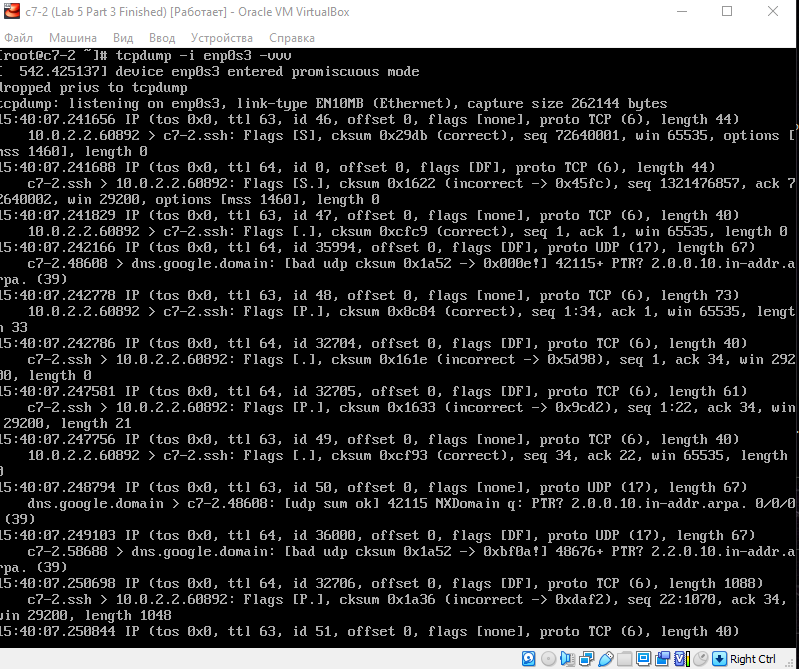




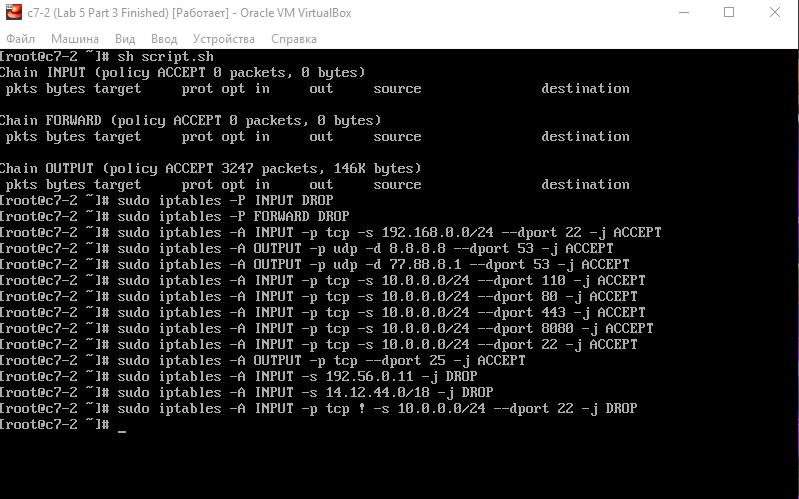






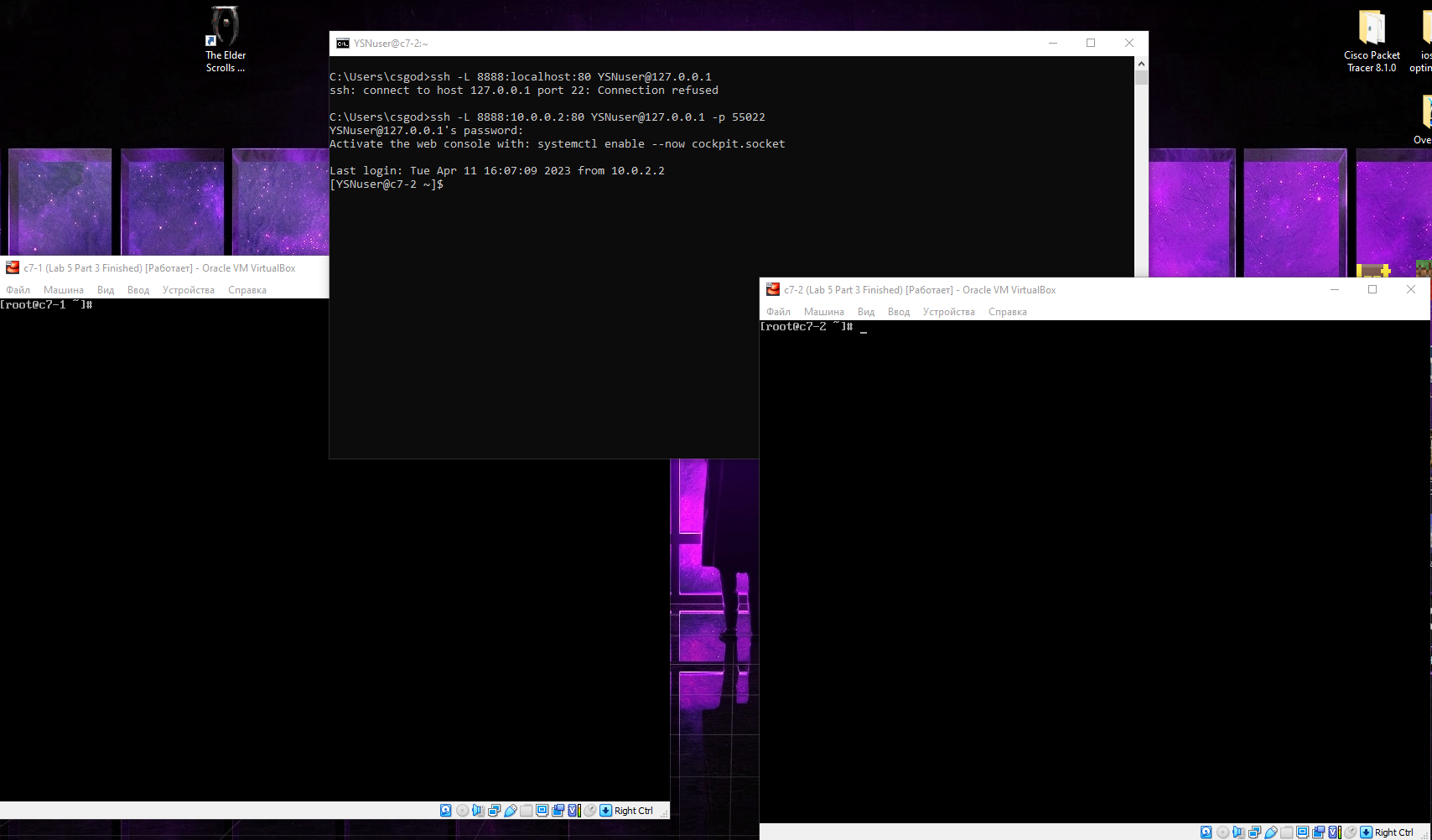


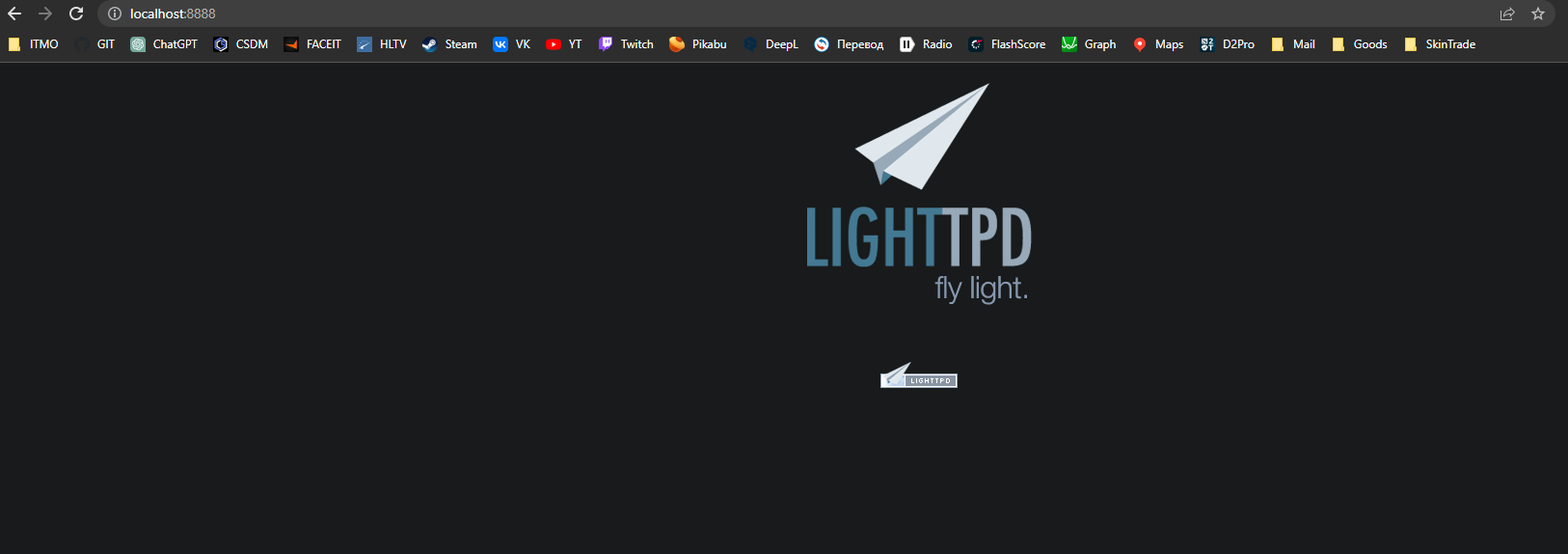
**Часть 6:**



**Часть 7:**

ssh –L 8888:10.0.0.2:80 [YSNuser@127.0.0.1](mailto:YSNuser@127.0.0.1) –p 55022





**Ответы на вопросы:**

1. Основное различие между SNAT и MASQUERADE заключается в том, что SNAT требует явного указания IP-адреса источника, в то время как MASQUERADE использует IP-адрес исходящего сетевого интерфейса. SNAT подходит, когда IP-адрес источника должен быть статичным и явно заданным, например, когда вы хотите убедиться, что трафик из определенной сети всегда идет с определенного IP-адреса. MASQUERADE обычно используется, когда IP-адрес источника может меняться или неизвестен, например, когда трафик идет с динамического IP-адреса, назначенного DHCP-сервером.
2. Таблицами по умолчанию в iptables являются filter, nat и mangle. Таблица filter используется для фильтрации пакетов на основе различных критериев, таких как адреса источника и назначения, порты и протоколы. Таблица nat используется для выполнения операций трансляции сетевых адресов (NAT), таких как перенаправление портов и маскировка. Таблица mangle используется для модификации пакетов, например, для изменения значения TTL или пометки пакетов для специальной обработки.
3. Чтобы добавить новую цепочку, нужно использовать следующую команду: iptables -N chain\_name - это создаст новую цепочку с именем chain\_name. Чтобы перенаправить трафик на новую цепочку, стоит использовать следующее правило: iptables -A INPUT -j chain\_name - это добавит правило к цепочке INPUT, которое перейдет к цепочке chain\_name для дальнейшей обработки.
4. Да, порядок правил в iptables имеет значение. Правила обрабатываются в порядке сверху вниз, и первое совпадающее правило определяет судьбу пакета. Поэтому важно расположить правила в правильном порядке, чтобы гарантировать, что они будут сопоставлены и обработаны так, как нужно. Например, если есть правило блокировки всего трафика, за которым следует правило разрешения трафика на определенный порт, правило блокировки будет иметь приоритет, а правило разрешения никогда не будет достигнуто.