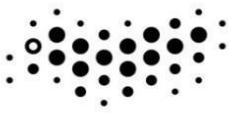
Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное учреждение высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Отчет

по лабораторной работе №6

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

Авторы: Юрпалов С. Н.,
Кошкин М.С.
Факультет: ИТиП
Группа: М33051

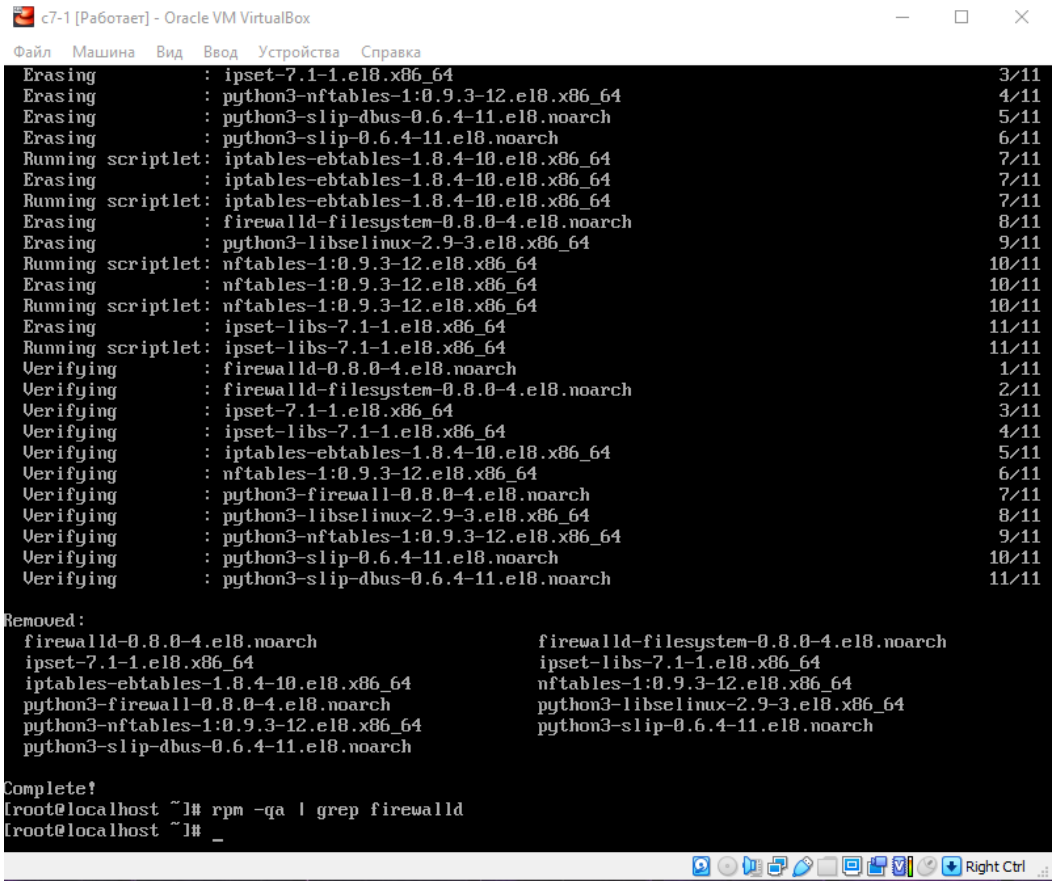


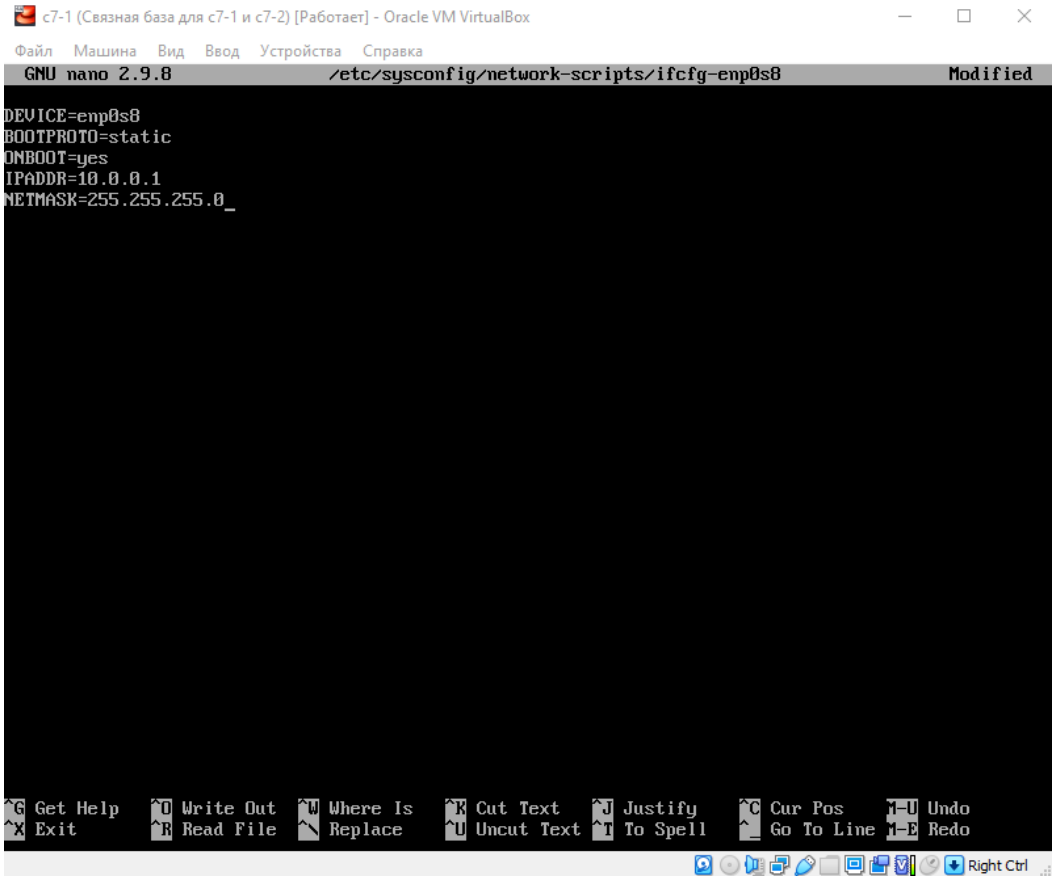
УНИВЕРСИТЕТ ИТМО

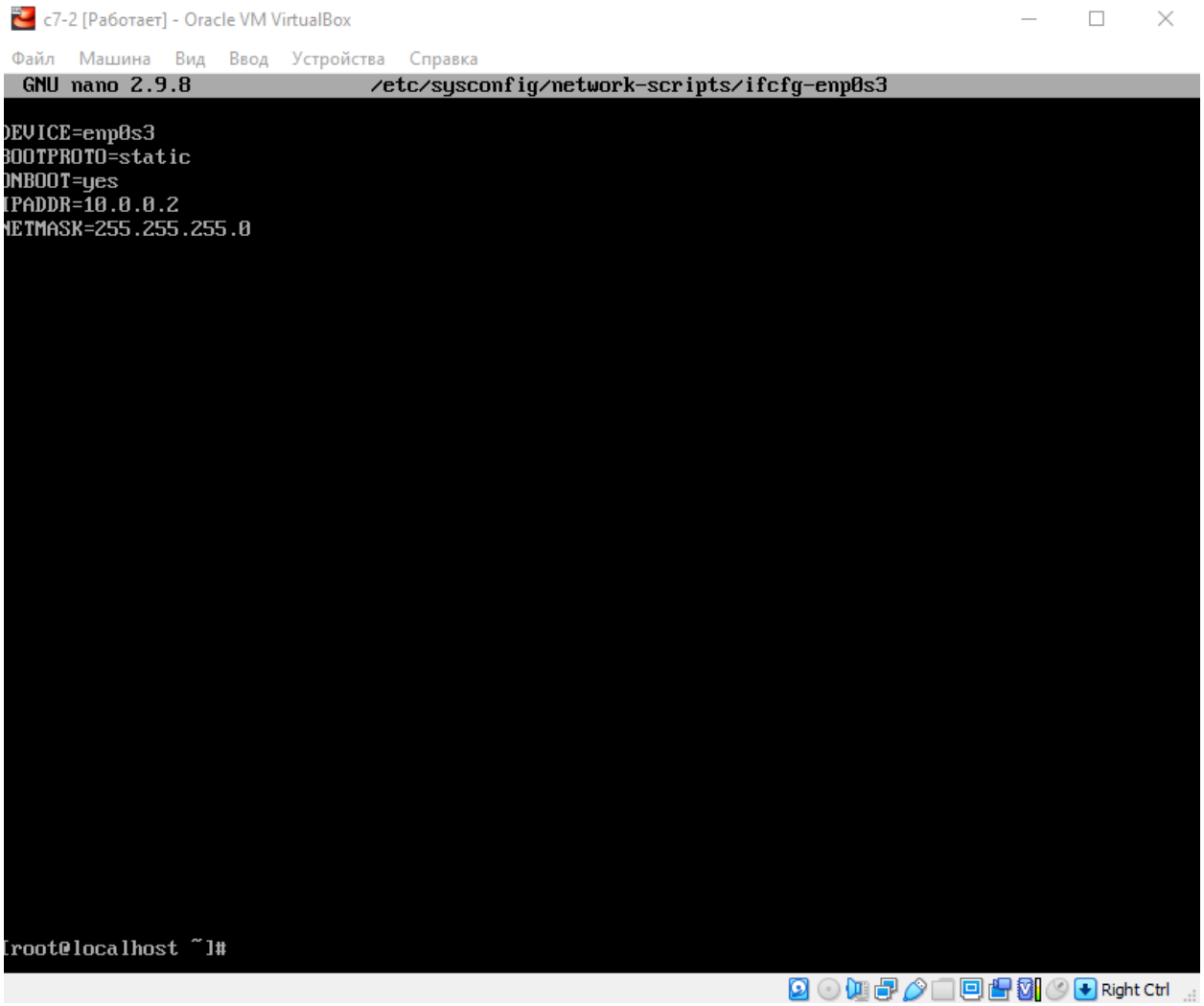
Санкт-Петербург 2023

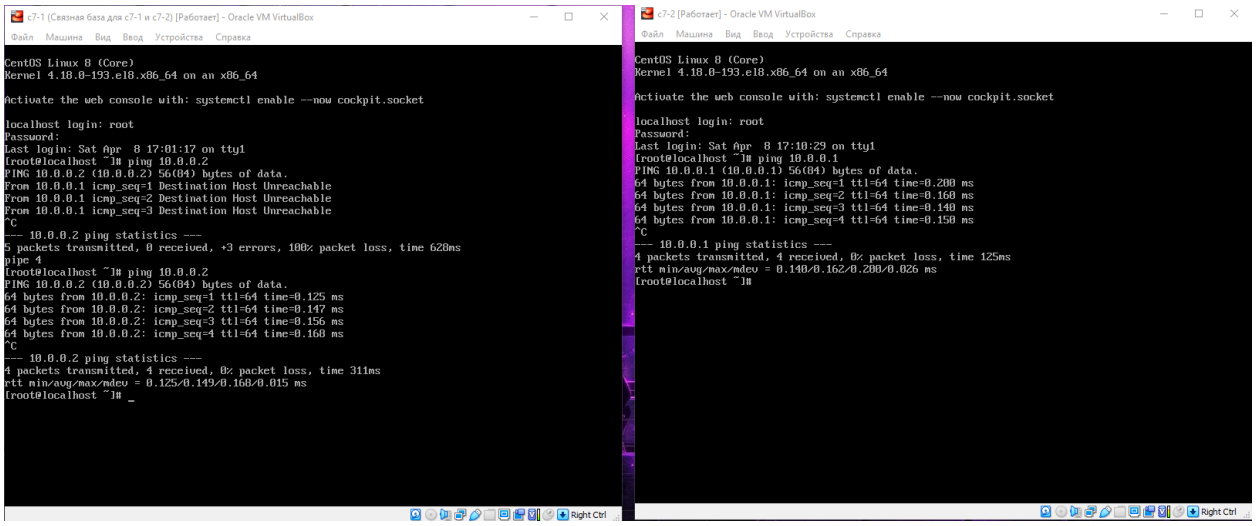
Ход работы

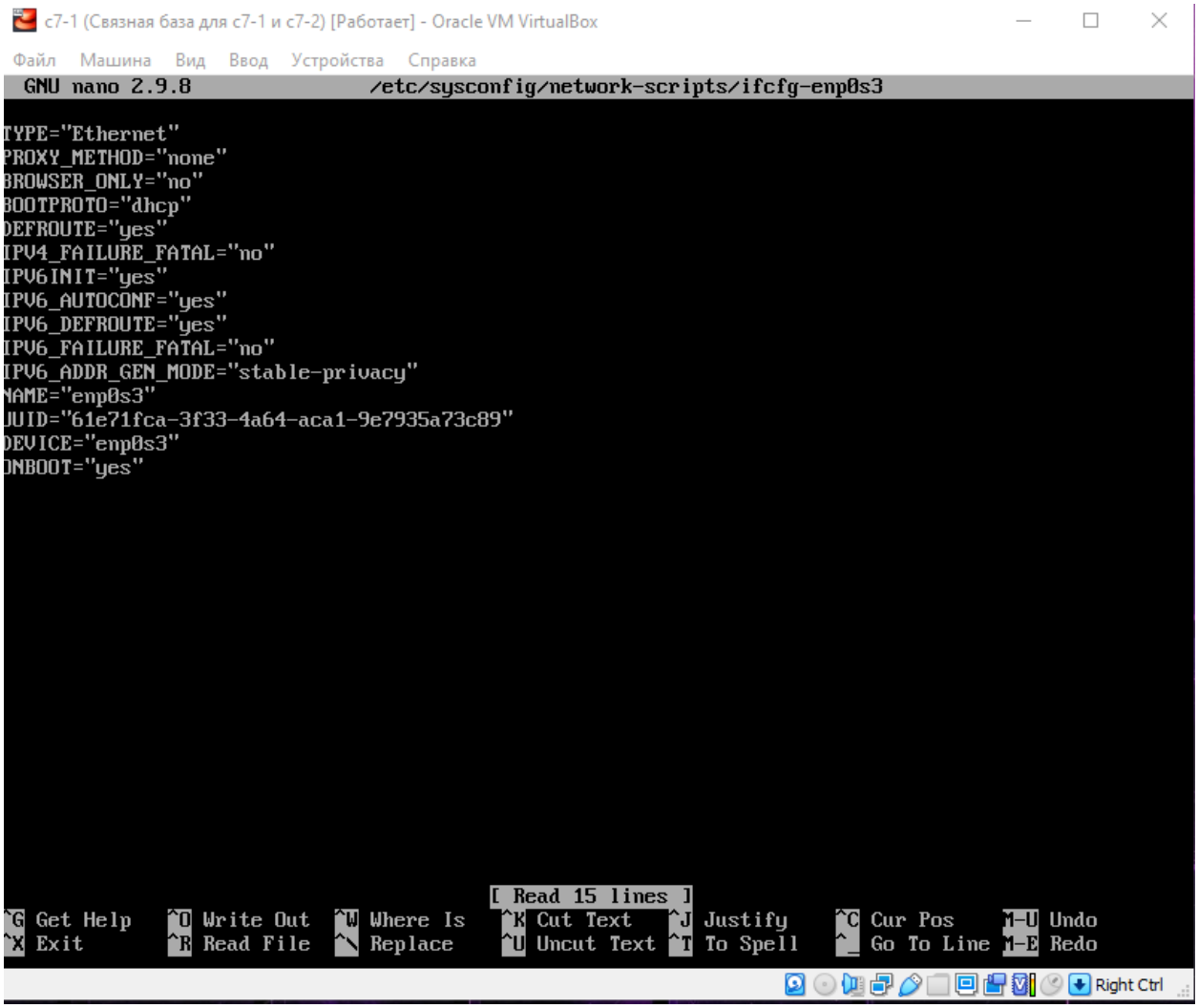
Часть 1:

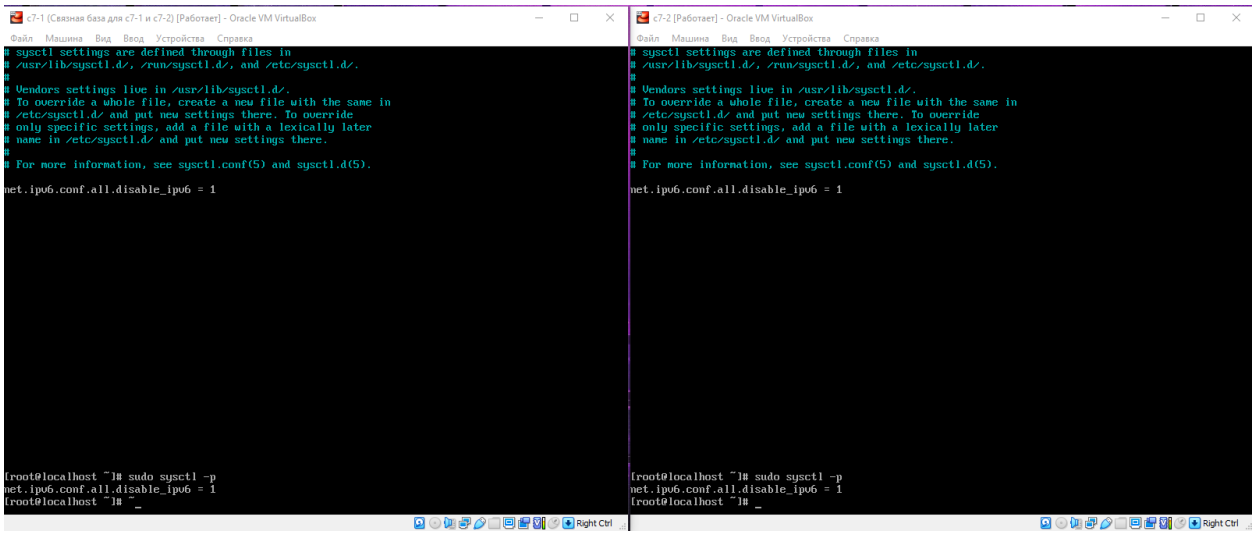


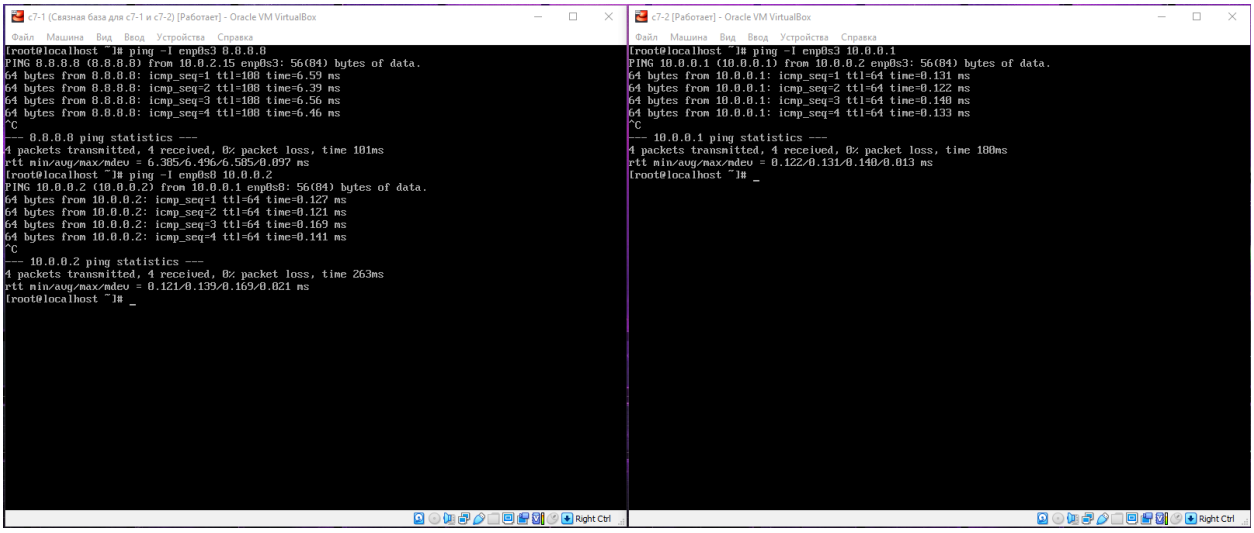


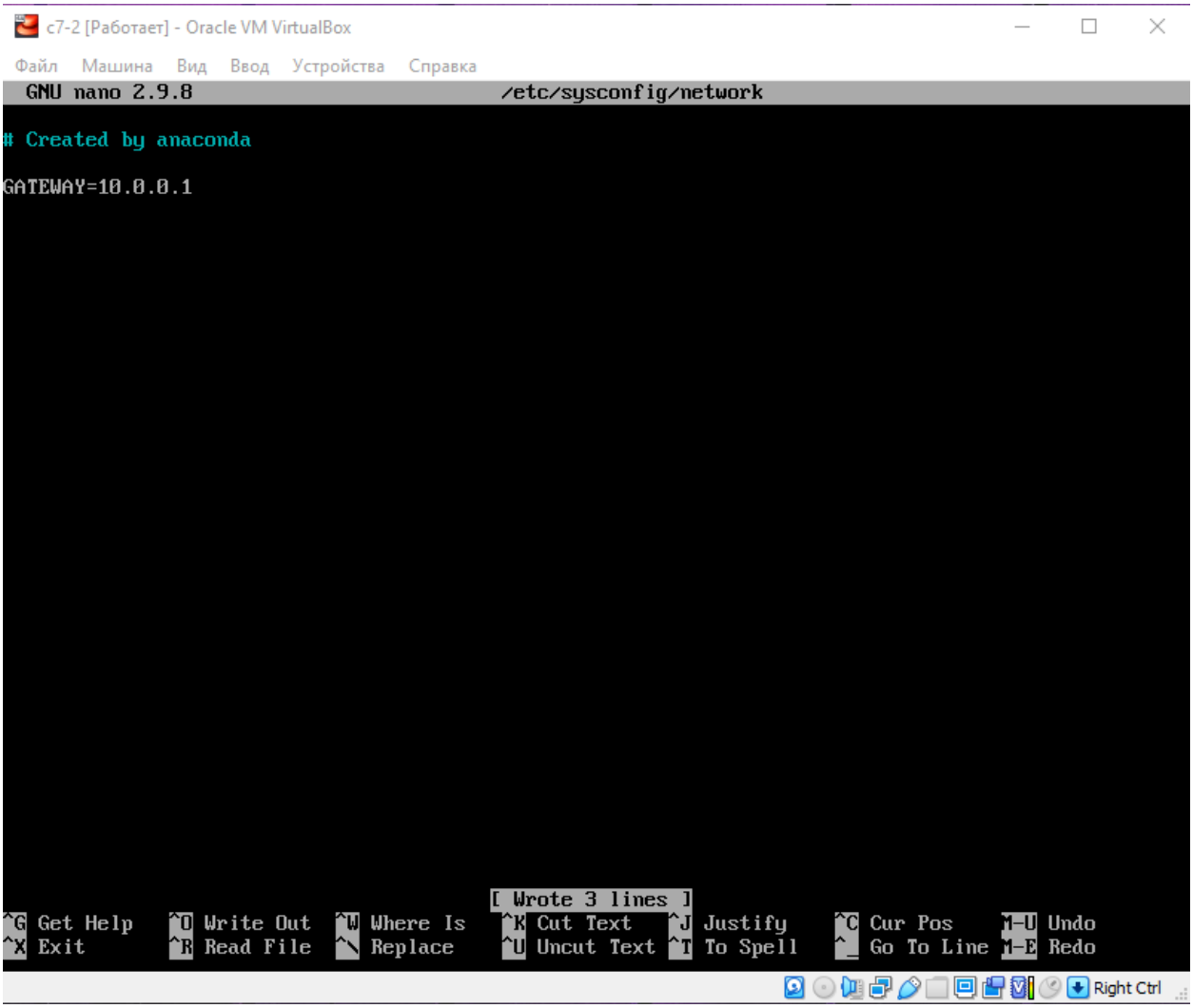

c7-2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
GNU nano 2.9.8 /etc/sysconfig/network-scripts/ifcfg-enp0s3
DEVICE=enp0s3
BOOTPROTO=static
ONBOOT=yes
IPADDR=10.0.0.2
NETMASK=255.255.255.0
[root@localhost ~]#
Right Ctrl


c7-1 (Связная база для c7-1 и c7-2) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
CentOS Linux 8 (Core)
Kernel 4.18.0-193.el8.x86_64 on an x86_64
Activate the web console with: systemctl enable --now cockpit.socket
localhost login: root
Password:
Last login: Sat Apr 8 17:01:17 on tty1
[root@localhost ~]# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
From 10.0.0.1 icmp_seq=1 Destination Host Unreachable
From 10.0.0.1 icmp_seq=2 Destination Host Unreachable
From 10.0.0.1 icmp_seq=3 Destination Host Unreachable
^C
--- 10.0.0.2 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 628ms
pipe 4
[root@localhost ~]# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.125 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.147 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.156 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.168 ms
^C
--- 10.0.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 311ms
rtt min/avg/max/mdev = 0.125/0.149/0.168/0.015 ms
[root@localhost ~]#
Right Ctrl
c7-2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
CentOS Linux 8 (Core)
Kernel 4.18.0-193.el8.x86_64 on an x86_64
Activate the web console with: systemctl enable --now cockpit.socket
localhost login: root
Password:
Last login: Sat Apr 8 17:10:29 on tty1
[root@localhost ~]# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.200 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.160 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.140 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.150 ms
^C
--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 125ms
rtt min/avg/max/mdev = 0.140/0.162/0.200/0.026 ms
[root@localhost ~]#
Right Ctrl


c7-1 (Связная база для c7-1 и c7-2) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
GNU nano 2.9.8 /etc/sysconfig/network-scripts/ifcfg-enp0s3
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="dhcp"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="enp0s3"
UUID="61e71fca-3f33-4a64-aca1-9e7935a73c89"
DEVICE="enp0s3"
ONBOOT="yes"
[Read 15 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo
Right Ctrl


sysctl settings are defined through files in
/usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
Vendors settings live in /usr/lib/sysctl.d/.
To override a whole file, create a new file with the same in
/etc/sysctl.d/ and put new settings there. To override
only specific settings, add a file with a lexically later
name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv6.conf.all.disable_ipv6 = 1
[root@localhost ~]# sudo sysctl -p
net.ipv6.conf.all.disable_ipv6 = 1
[root@localhost ~]#
Right Ctrl



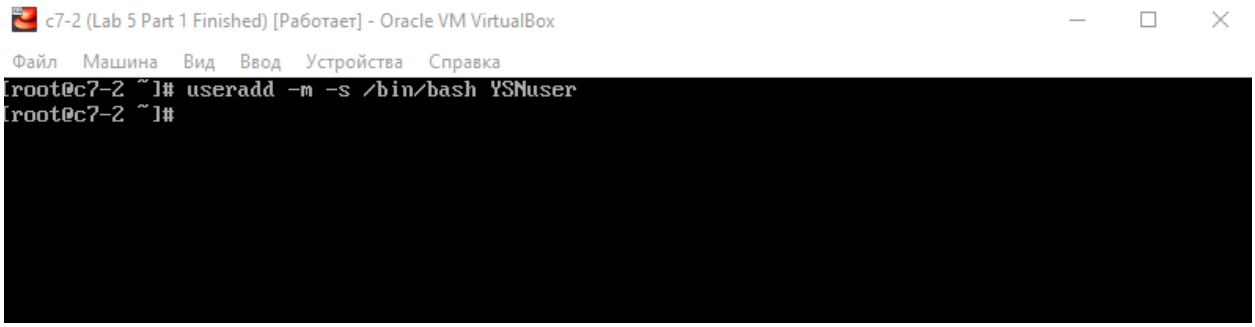


/etc/sysctl.conf

net.ipv4.ip_forward = 1

Часть 2:

sudo passwd YSNuser 12345



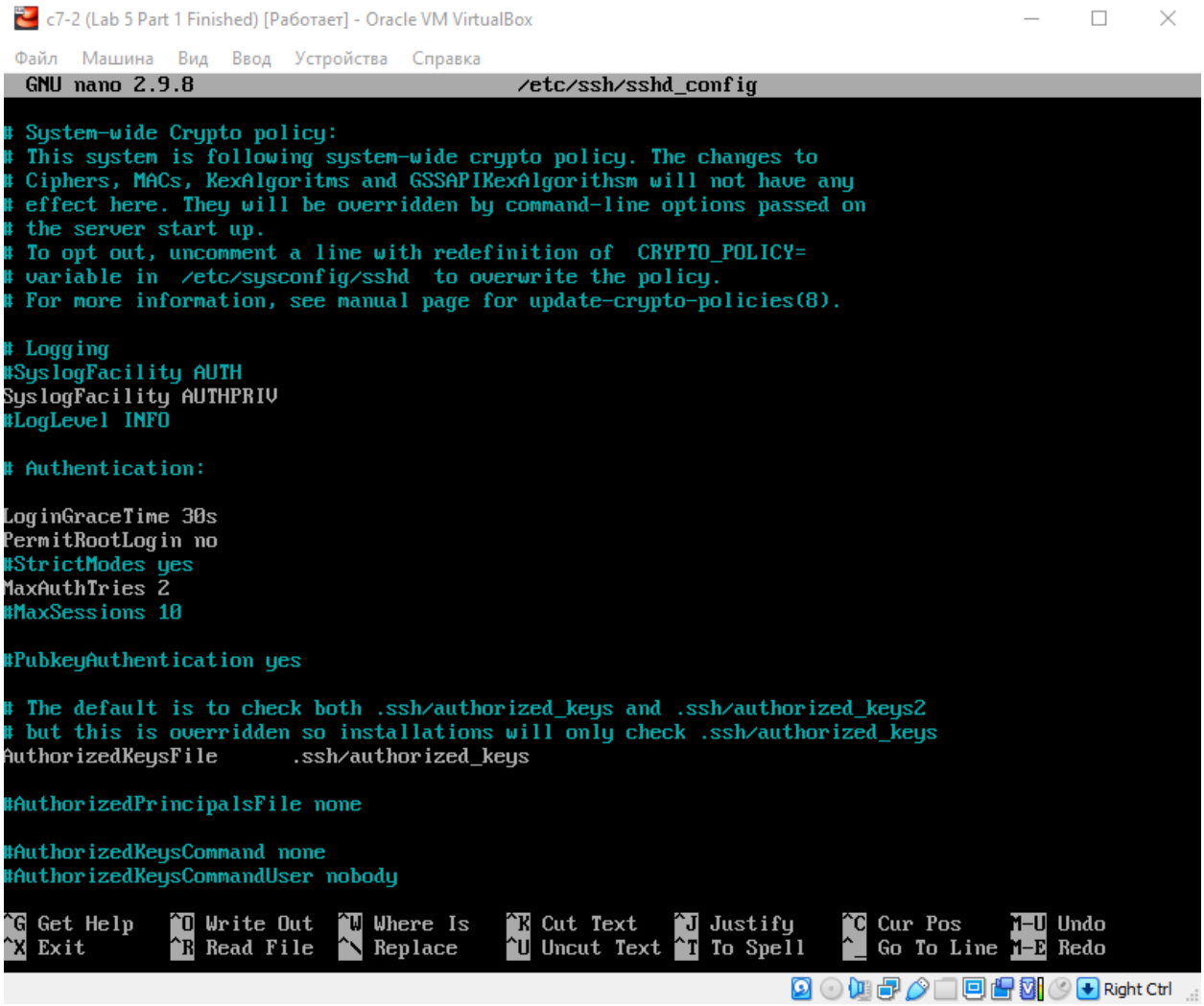
/etc/ssh/sshd_config

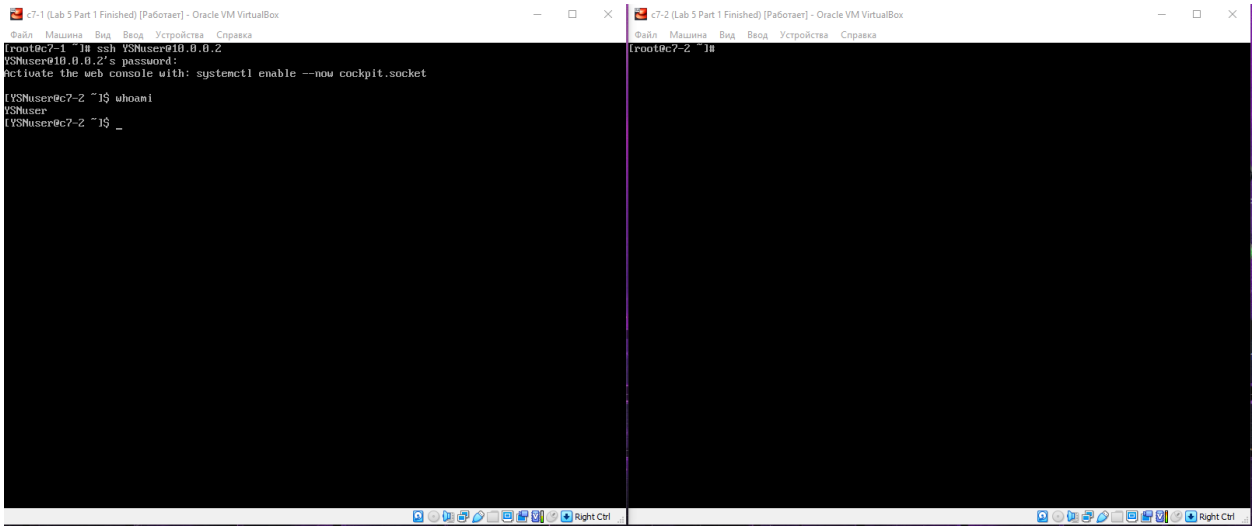
PermitRootLogin no

MaxAuthTries 2

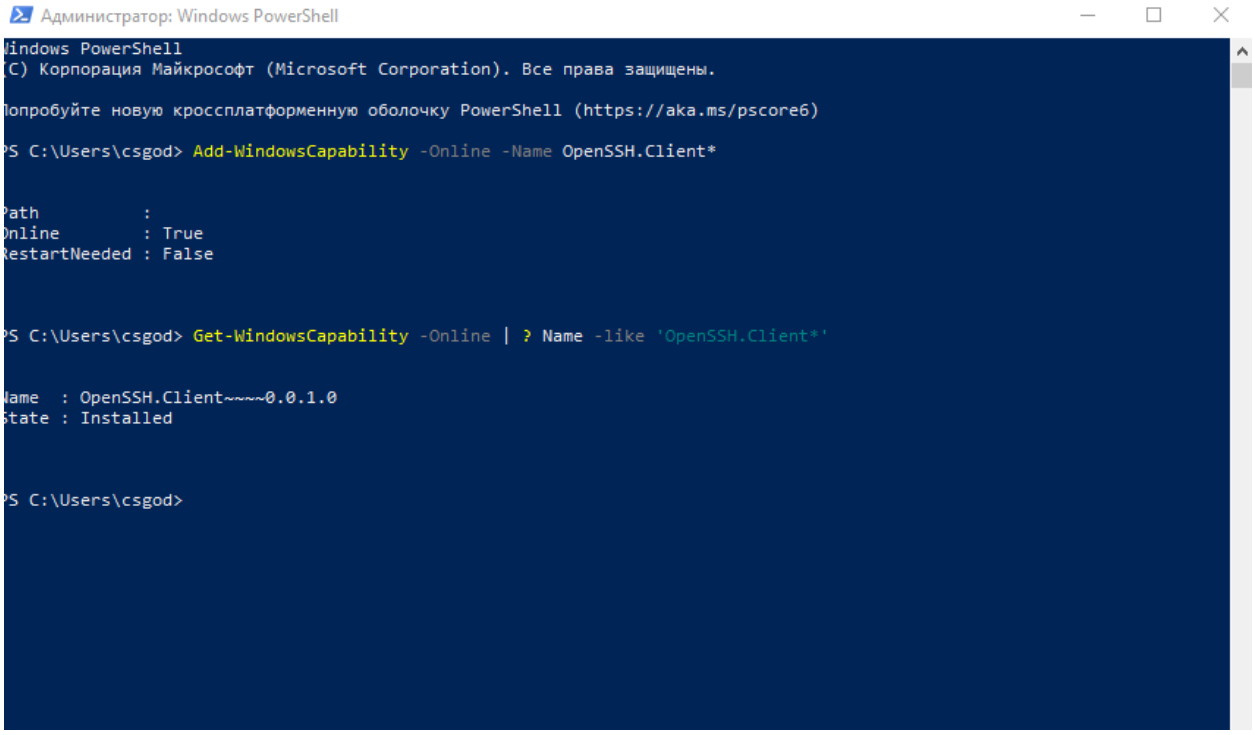
LoginGraceTime 30s

UseDNS no




c7-1 (Lab 5 Part 1 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
[root@c7-1 ~]# ssh YSNuser@10.0.0.2
YSNuser@10.0.0.2's password:
Activate the web console with: systemctl enable --now cockpit.socket
[YSNuser@c7-2 ~]$ whoami
YSNuser
[YSNuser@c7-2 ~]$
Right Ctrl
c7-2 (Lab 5 Part 1 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
[root@c7-2 ~]#
Right Ctrl

Часть 3:

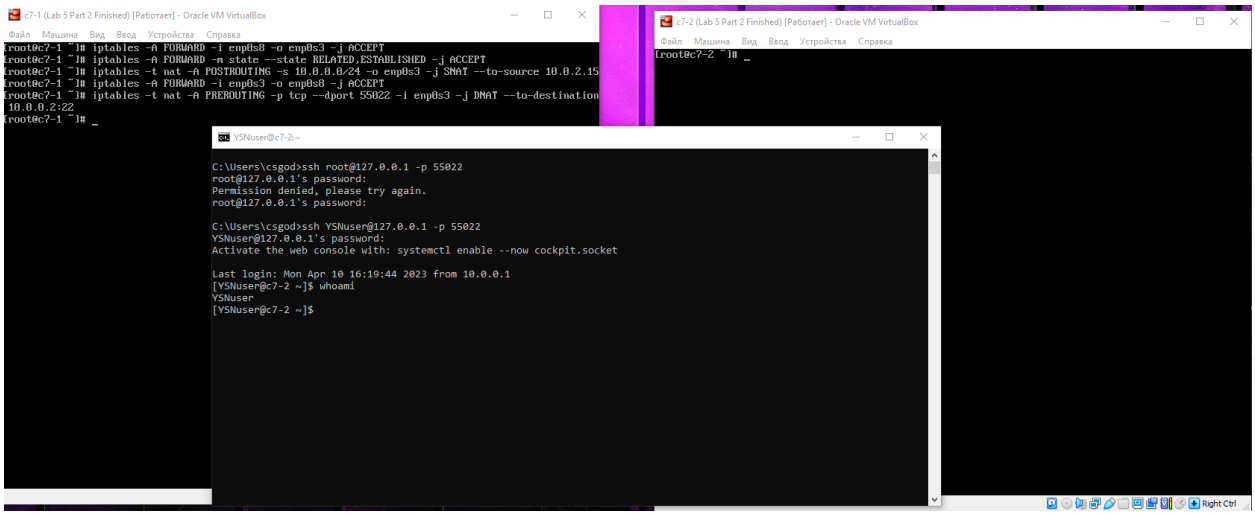

Администратор: Windows PowerShell
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)
PS C:\Users\csgod> Add-WindowsCapability -Online -Name OpenSSH.Client*
Path :
Online : True
RestartNeeded : False
PS C:\Users\csgod> Get-WindowsCapability -Online | ? Name -like 'OpenSSH.Client*'
Name : OpenSSH.Client~~~~0.0.1.0
State : Installed
PS C:\Users\csgod>

c7-1 (Lab 5 Part 2 Finished) [Работает] - Oracle VM VirtualBox

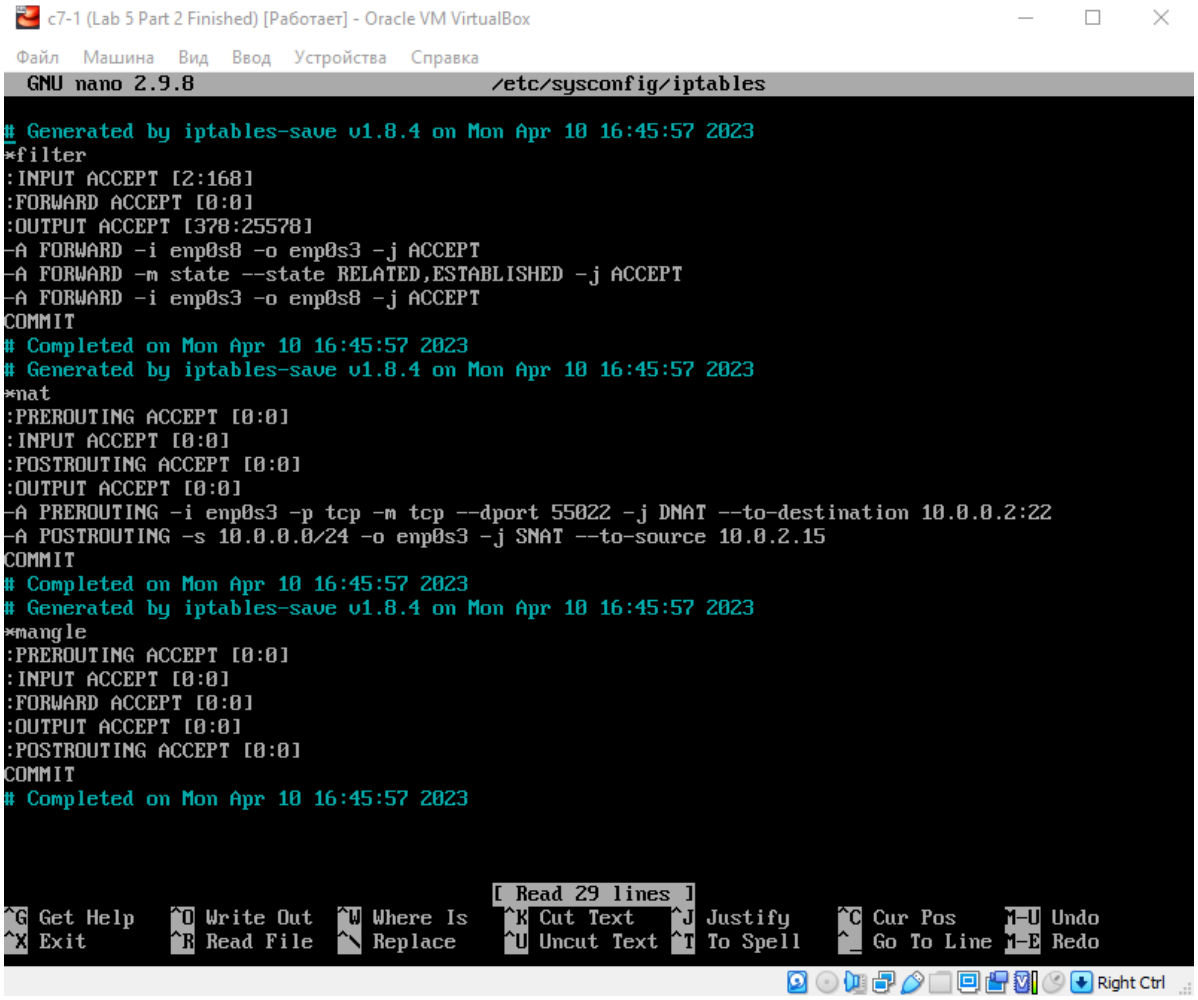
Файл Машина Вид Ввод Устройства Справка

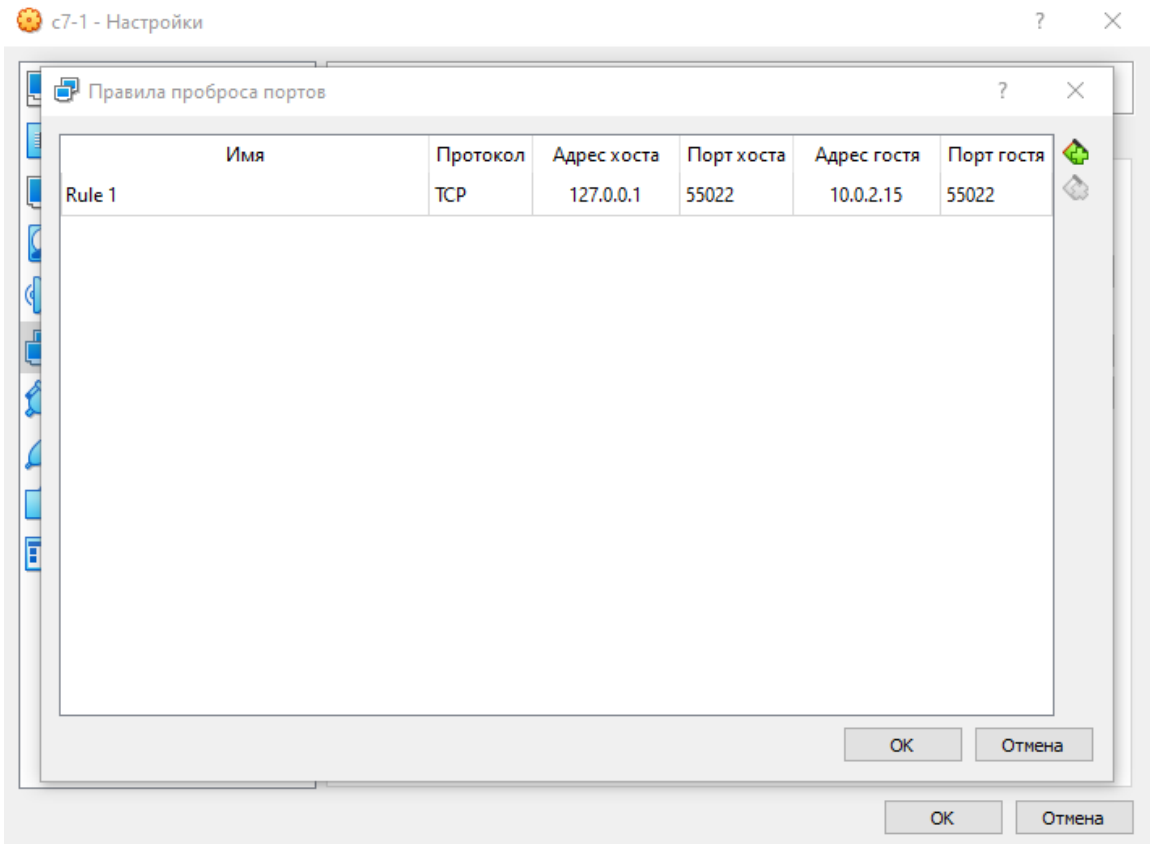
```
 GNU nano 2.9.8                          script.sh

#!/bin/bash

iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -t nat -F
iptables -t mangle -F
iptables -F
iptables -X

iptables -nvL

                        [ Read 11 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Linter ^_ Go To Line M-E Redo
```

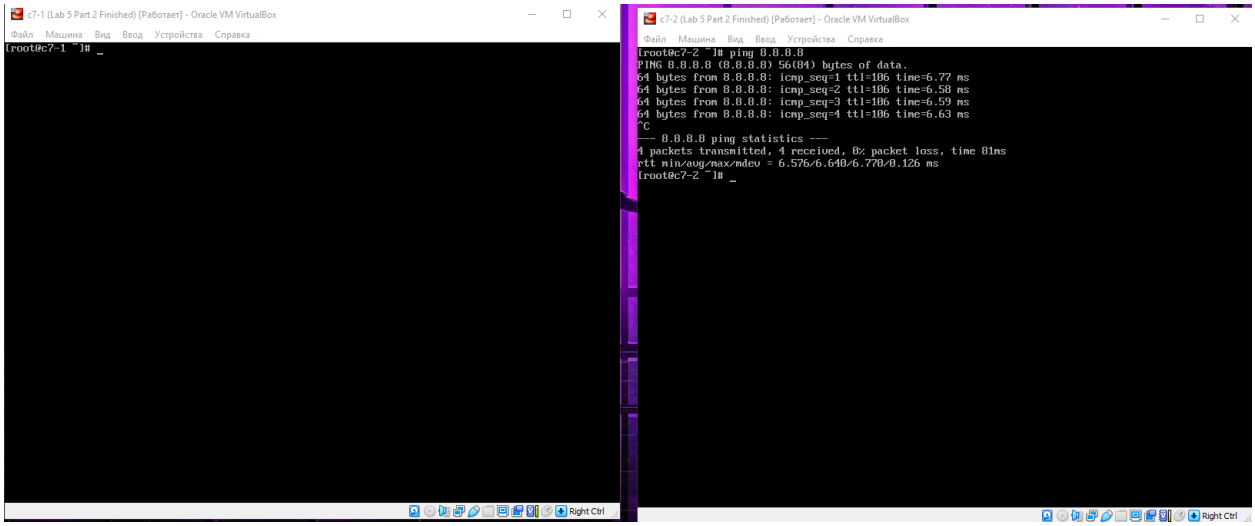
Right Ctrl



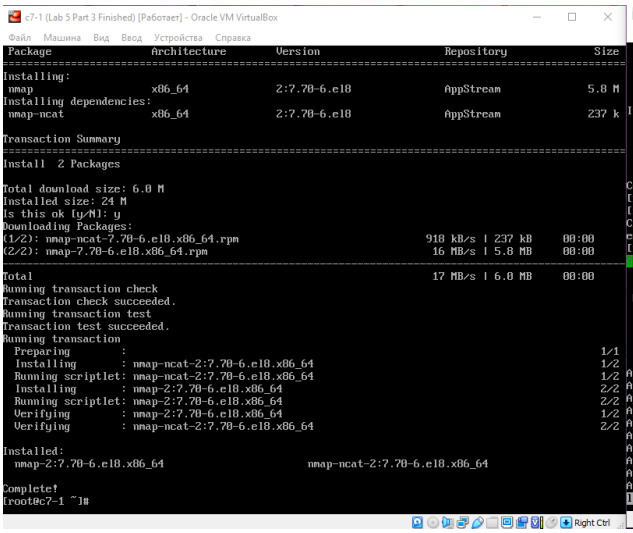
sudo iptables-save > /etc/sysconfig/iptables

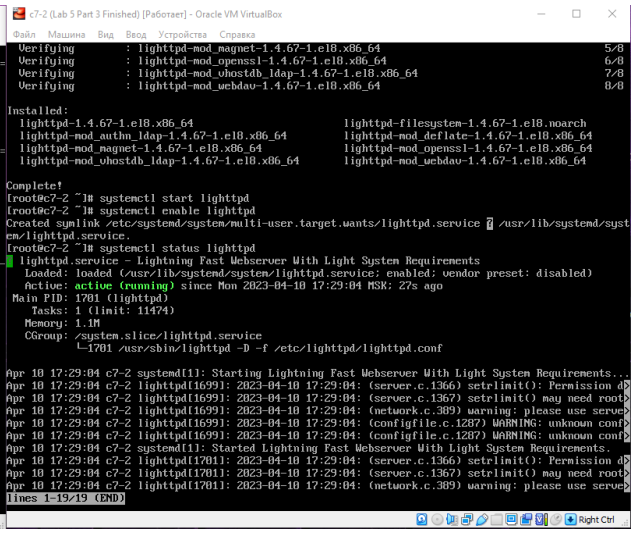


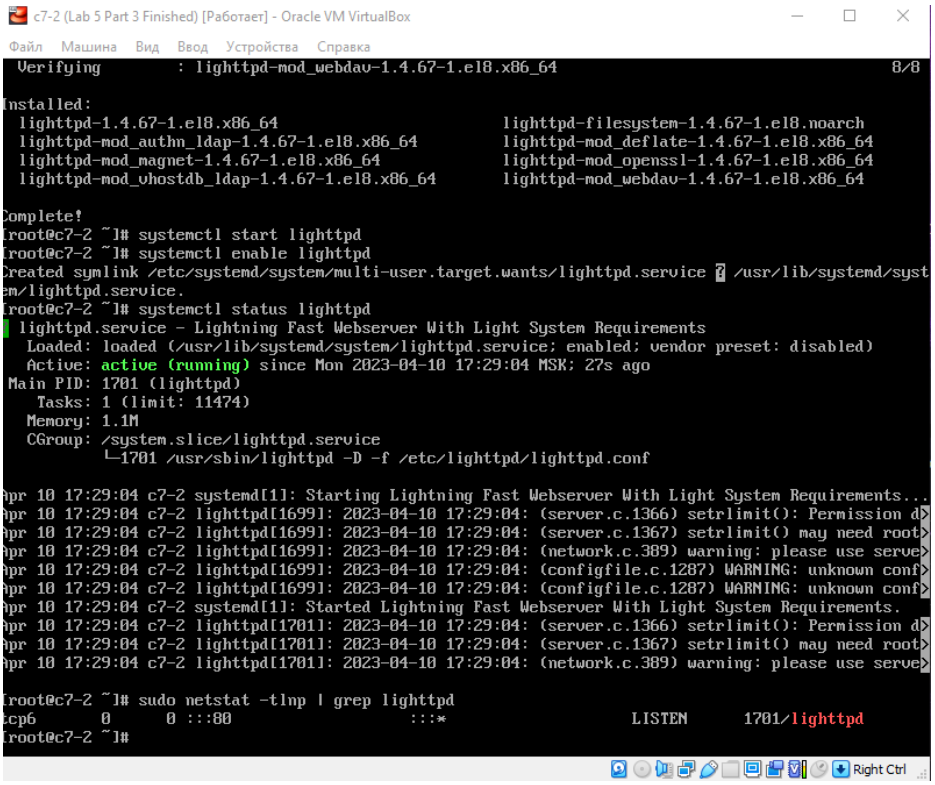



c7-1 (Lab 5 Part 2 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
[root@c7-1 ~]# _
Right Ctrl
c7-2 (Lab 5 Part 2 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
[root@c7-2 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=106 time=6.77 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=106 time=6.58 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=106 time=6.59 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=106 time=6.63 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 81ms
rtt min/avg/max/mdev = 6.576/6.640/6.770/0.126 ms
[root@c7-2 ~]# _
Right Ctrl

Часть 4:


c7-1 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Package Architecture Version Repository Size
Installing:
nmap x86_64 2:7.70-6.el8 AppStream 5.8 M
Installing dependencies:
nmap-ncat x86_64 2:7.70-6.el8 AppStream 237 k
Transaction Summary
Install 2 Packages
Total download size: 6.0 M
Installed size: 24 M
Is this ok [y/N]: y
Downloading Packages:
(1/2): nmap-ncat-7.70-6.el8.x86_64.rpm 918 kB/s | 237 kB 00:00
(2/2): nmap-7.70-6.el8.x86_64.rpm 16 MB/s | 5.8 MB 00:00
Total 17 MB/s | 6.0 MB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : nmap-ncat-2:7.70-6.el8.x86_64 1/2
Running scriptlet: nmap-ncat-2:7.70-6.el8.x86_64 1/2
Installing : nmap-2:7.70-6.el8.x86_64 2/2
Running scriptlet: nmap-2:7.70-6.el8.x86_64 2/2
Verifying : nmap-2:7.70-6.el8.x86_64 1/2
Verifying : nmap-ncat-2:7.70-6.el8.x86_64 2/2
Installed:
nmap-2:7.70-6.el8.x86_64 nmap-ncat-2:7.70-6.el8.x86_64
Complete!
[root@c7-1 ~]#
Right Ctrl


c7-2 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Verifying : lighttpd-mod_magnet-1.4.67-1.el8.x86_64 5/8
Verifying : lighttpd-mod_openssl-1.4.67-1.el8.x86_64 6/8
Verifying : lighttpd-mod_vhostdb_ldap-1.4.67-1.el8.x86_64 7/8
Verifying : lighttpd-mod_webdav-1.4.67-1.el8.x86_64 8/8
Installed:
lighttpd-1.4.67-1.el8.x86_64 lighttpd-filesystem-1.4.67-1.el8.noarch
lighttpd-mod_authn_ldap-1.4.67-1.el8.x86_64 lighttpd-mod_deflate-1.4.67-1.el8.x86_64
lighttpd-mod_magnet-1.4.67-1.el8.x86_64 lighttpd-mod_openssl-1.4.67-1.el8.x86_64
lighttpd-mod_vhostdb_ldap-1.4.67-1.el8.x86_64 lighttpd-mod_webdav-1.4.67-1.el8.x86_64
Complete!
[root@c7-2 ~]# systemctl start lighttpd
[root@c7-2 ~]# systemctl enable lighttpd
Created symlink /etc/systemd/system/multi-user.target.wants/lighttpd.service ? /usr/lib/systemd/system/lighttpd.service.
[root@c7-2 ~]# systemctl status lighttpd
lighttpd.service - Lighttning Fast Webserver With Light System Requirements
Loaded: loaded (/usr/lib/systemd/system/lighttpd.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2023-04-10 17:29:04 MSK; 27s ago
Main PID: 1701 (lighttpd)
Tasks: 1 (limit: 11474)
Memory: 1.1M
CGroup: /system.slice/lighttpd.service
└─1701 /usr/sbin/lighttpd -D -f /etc/lighttpd/lighttpd.conf
Apr 10 17:29:04 c7-2 systemd[1]: Starting Lightning Fast Webserver With Light System Requirements...
Apr 10 17:29:04 c7-2 lighttpd[1699]: 2023-04-10 17:29:04: (server.c.1366) setrlimit(): Permission d
Apr 10 17:29:04 c7-2 lighttpd[1699]: 2023-04-10 17:29:04: (server.c.1367) setrlimit() may need root
Apr 10 17:29:04 c7-2 lighttpd[1699]: 2023-04-10 17:29:04: (network.c.389) warning: please use serve
Apr 10 17:29:04 c7-2 lighttpd[1699]: 2023-04-10 17:29:04: (configfile.c.1287) WARNING: unknown conf
Apr 10 17:29:04 c7-2 lighttpd[1699]: 2023-04-10 17:29:04: (configfile.c.1287) WARNING: unknown conf
Apr 10 17:29:04 c7-2 systemd[1]: Started Lightning Fast Webserver With Light System Requirements.
Apr 10 17:29:04 c7-2 lighttpd[1701]: 2023-04-10 17:29:04: (server.c.1366) setrlimit(): Permission d
Apr 10 17:29:04 c7-2 lighttpd[1701]: 2023-04-10 17:29:04: (server.c.1367) setrlimit() may need root
Apr 10 17:29:04 c7-2 lighttpd[1701]: 2023-04-10 17:29:04: (network.c.389) warning: please use serve
lines 1-19/19 (END)
Right Ctrl


c7-2 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Verifying : lighttpd-mod_webdav-1.4.67-1.el8.x86_64 8/8
Installed:
lighttpd-1.4.67-1.el8.x86_64 lighttpd-filesystem-1.4.67-1.el8.noarch
lighttpd-mod_authn_ldap-1.4.67-1.el8.x86_64 lighttpd-mod_deflate-1.4.67-1.el8.x86_64
lighttpd-mod_magnet-1.4.67-1.el8.x86_64 lighttpd-mod_openssl-1.4.67-1.el8.x86_64
lighttpd-mod_vhostdb_ldap-1.4.67-1.el8.x86_64 lighttpd-mod_webdav-1.4.67-1.el8.x86_64
Complete!
[root@c7-2 ~]# systemctl start lighttpd
[root@c7-2 ~]# systemctl enable lighttpd
Created symlink /etc/systemd/system/multi-user.target.wants/lighttpd.service ? /usr/lib/systemd/system/lighttpd.service.
[root@c7-2 ~]# systemctl status lighttpd
lighttpd.service - Lighttning Fast Webserver With Light System Requirements
Loaded: loaded (/usr/lib/systemd/system/lighttpd.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2023-04-10 17:29:04 MSK; 27s ago
Main PID: 1701 (lighttpd)
Tasks: 1 (limit: 11474)
Memory: 1.1M
CGroup: /system.slice/lighttpd.service
└─1701 /usr/sbin/lighttpd -D -f /etc/lighttpd/lighttpd.conf
Apr 10 17:29:04 c7-2 systemd[1]: Starting Lightning Fast Webserver With Light System Requirements...
Apr 10 17:29:04 c7-2 lighttpd[1699]: 2023-04-10 17:29:04: (server.c.1366) setrlimit(): Permission d
Apr 10 17:29:04 c7-2 lighttpd[1699]: 2023-04-10 17:29:04: (server.c.1367) setrlimit() may need root
Apr 10 17:29:04 c7-2 lighttpd[1699]: 2023-04-10 17:29:04: (network.c.389) warning: please use serve
Apr 10 17:29:04 c7-2 lighttpd[1699]: 2023-04-10 17:29:04: (configfile.c.1287) WARNING: unknown conf
Apr 10 17:29:04 c7-2 lighttpd[1699]: 2023-04-10 17:29:04: (configfile.c.1287) WARNING: unknown conf
Apr 10 17:29:04 c7-2 systemd[1]: Started Lightning Fast Webserver With Light System Requirements.
Apr 10 17:29:04 c7-2 lighttpd[1701]: 2023-04-10 17:29:04: (server.c.1366) setrlimit(): Permission d
Apr 10 17:29:04 c7-2 lighttpd[1701]: 2023-04-10 17:29:04: (server.c.1367) setrlimit() may need root
Apr 10 17:29:04 c7-2 lighttpd[1701]: 2023-04-10 17:29:04: (network.c.389) warning: please use serve
[root@c7-2 ~]# sudo netstat -tlnp | grep lighttpd
tcp6 0 0 :::80 :::* LISTEN 1701/lighttpd
[root@c7-2 ~]#
Right Ctrl

c7-2 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

```
 GNU nano 2.9.8                        /etc/lighttpd/lighttpd.conf

include conf_dir + "/modules.conf"

##
############################################################################

############################################################################
##
##  Basic Configuration
## ---------------------
##
server.port = 80

##
## Use IPv6?
##
server.use-ipv6 = "disable"
```

c7-1 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox

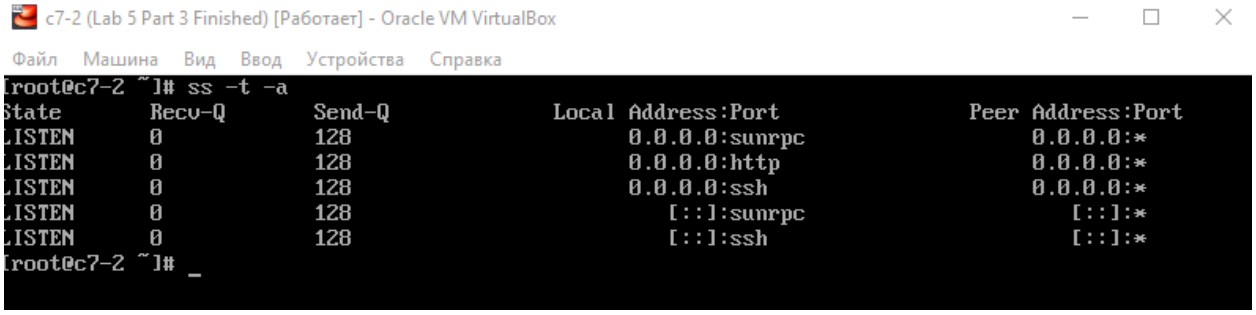
Файл Машина Вид Ввод Устройства Справка

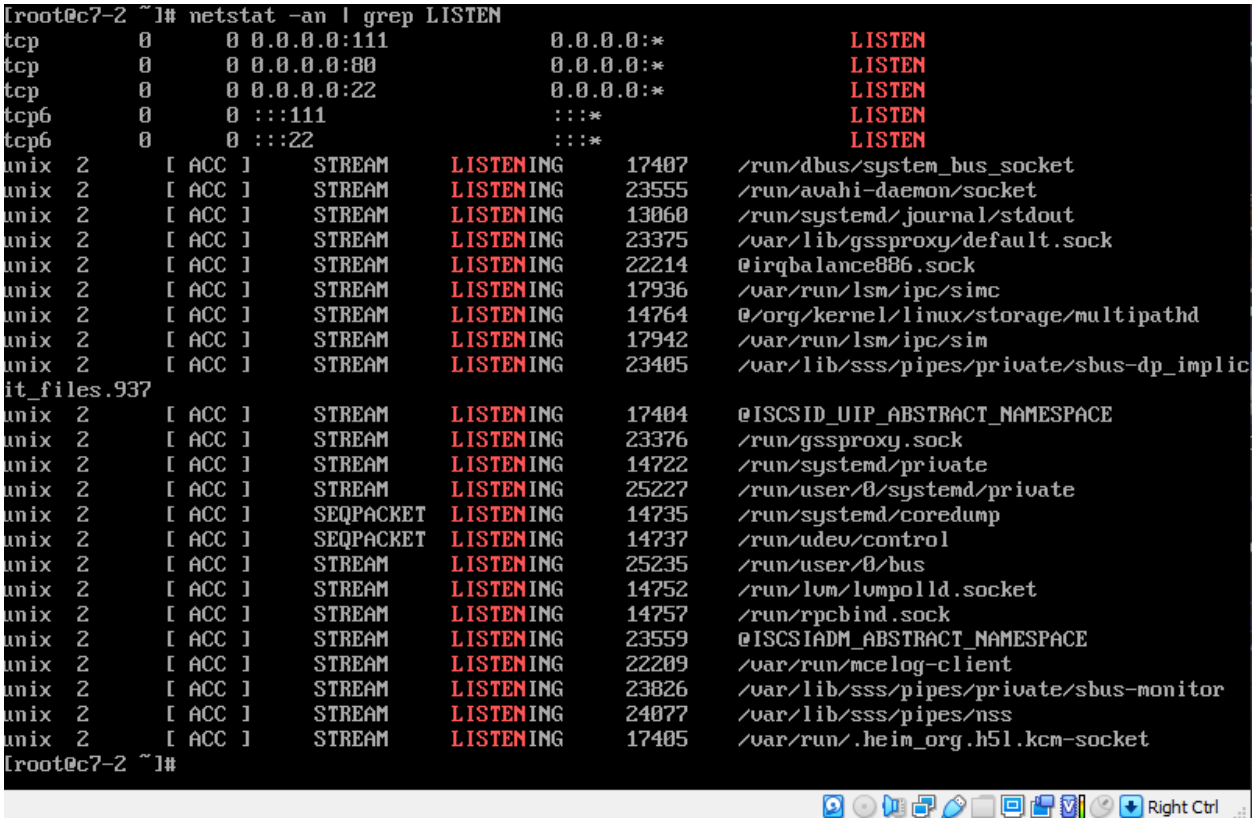
```
[root@c7-1 ~]# sudo nmap 10.0.0.2
Starting Nmap 7.70 ( https://nmap.org ) at 2023-04-10 17:37 MSK
Nmap scan report for 10.0.0.2
Host is up (0.00012s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  lighttpd
MAC Address: 08:00:27:36:EE:E7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 10.15 seconds
[root@c7-1 ~]#
```

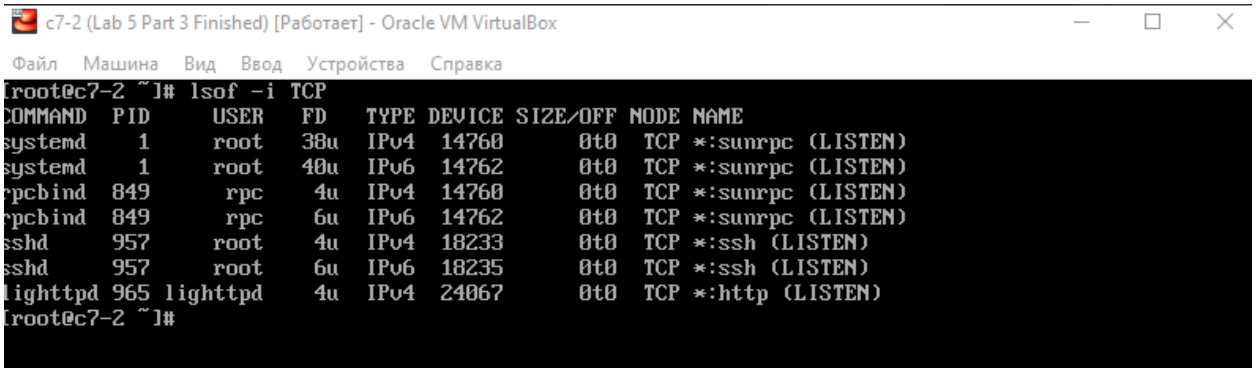
Right Ctrl

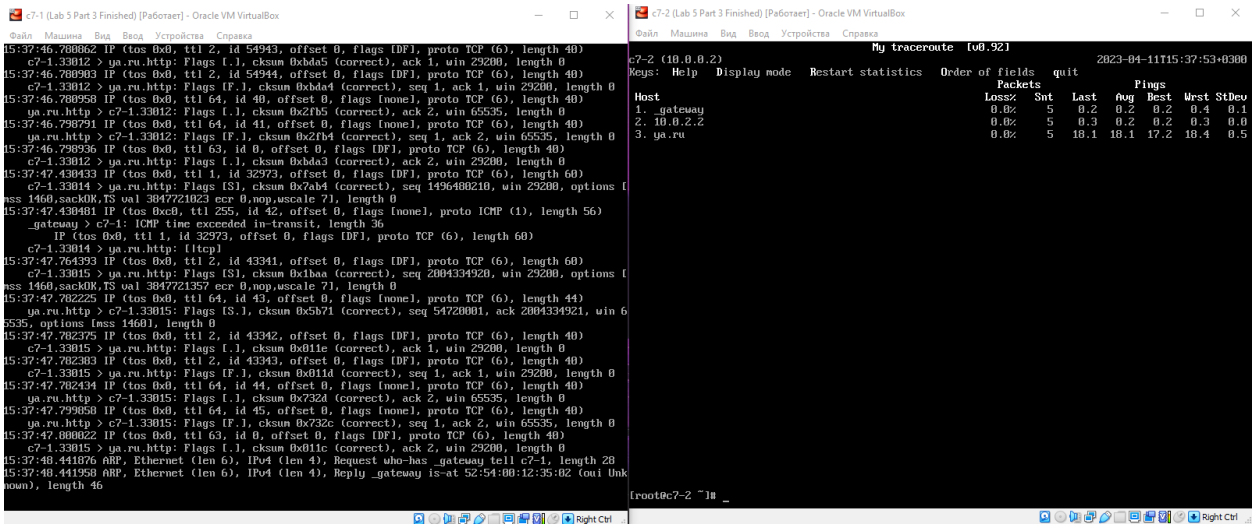

c7-1 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Powered by lighttpd
LIGHTTPD - fly light.
Powered by GNU/Linux
Powered by Lighttpd
Image http://10.0.0.2/light_logo.png
[------]
Right Ctrl

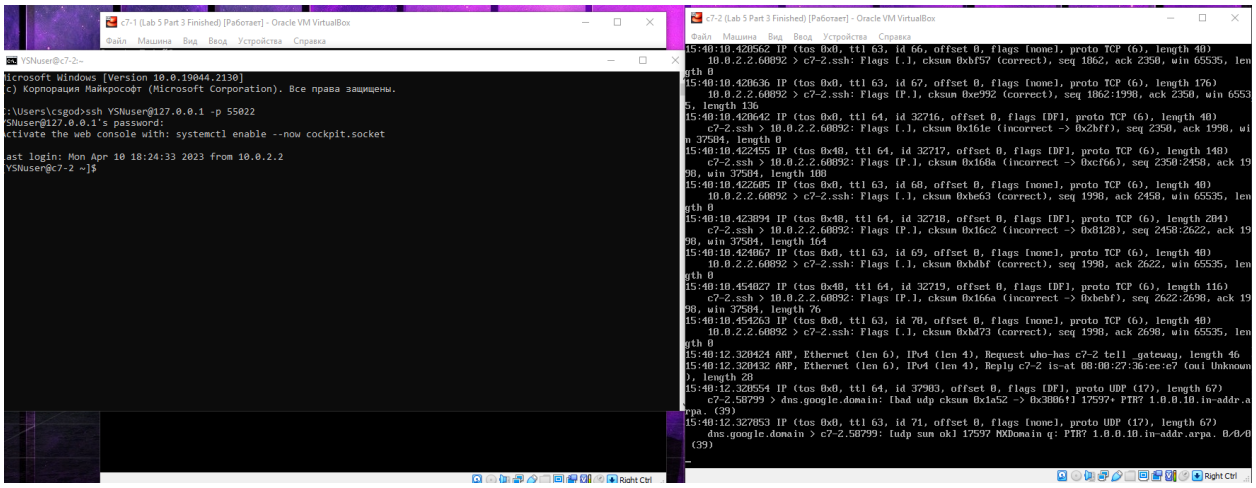
Часть 5:

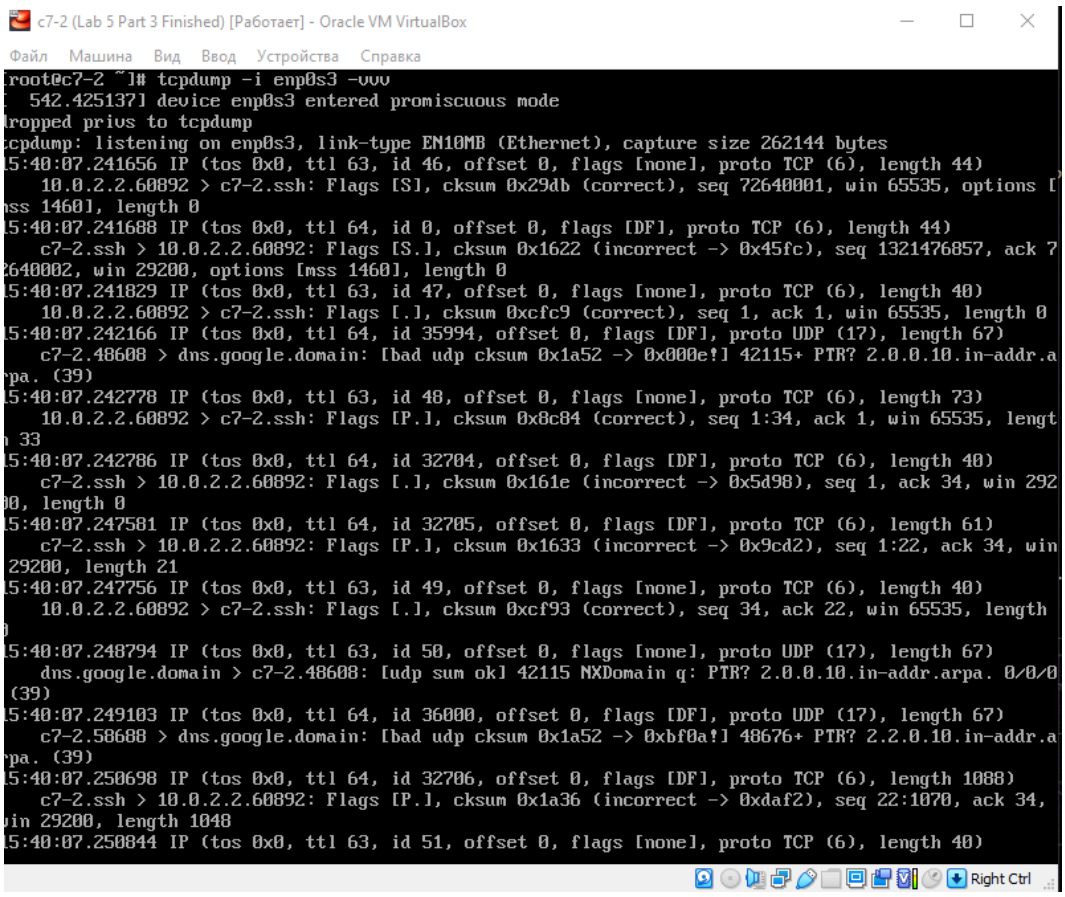

c7-2 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
[root@c7-2 ~]# ss -t -a
State Recv-Q Send-Q Local Address:Port Peer Address:Port
LISTEN 0 128 0.0.0.0:sunrpc 0.0.0.0:*
LISTEN 0 128 0.0.0.0:http 0.0.0.0:*
LISTEN 0 128 0.0.0.0:ssh 0.0.0.0:*
LISTEN 0 128 [::]:sunrpc [::]:*
LISTEN 0 128 [::]:ssh [::]:*
[root@c7-2 ~]#


[root@c7-2 ~]# netstat -an | grep LISTEN
tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp6 0 0 :::111 :::* LISTEN
tcp6 0 0 :::22 :::* LISTEN
unix 2 [ACC] STREAM LISTENING 17407 /run/dbus/system_bus_socket
unix 2 [ACC] STREAM LISTENING 23555 /run/avahi-daemon/socket
unix 2 [ACC] STREAM LISTENING 13060 /run/systemd/journal/stdout
unix 2 [ACC] STREAM LISTENING 23375 /var/lib/gssproxy/default.sock
unix 2 [ACC] STREAM LISTENING 22214 @irqbalance886.sock
unix 2 [ACC] STREAM LISTENING 17936 /var/run/lsm/ipc/simc
unix 2 [ACC] STREAM LISTENING 14764 @/org/kernel/linux/storage/multipathd
unix 2 [ACC] STREAM LISTENING 17942 /var/run/lsm/ipc/sim
unix 2 [ACC] STREAM LISTENING 23405 /var/lib/sss/pipes/private/sbus-dp_implic
it_files.937
unix 2 [ACC] STREAM LISTENING 17404 @ISCSID_UIP_ABSTRACT_NAMESPACE
unix 2 [ACC] STREAM LISTENING 23376 /run/gssproxy.sock
unix 2 [ACC] STREAM LISTENING 14722 /run/systemd/private
unix 2 [ACC] STREAM LISTENING 25227 /run/user/0/systemd/private
unix 2 [ACC] SEQPACKET LISTENING 14735 /run/systemd/coredump
unix 2 [ACC] SEQPACKET LISTENING 14737 /run/udev/control
unix 2 [ACC] STREAM LISTENING 25235 /run/user/0/bus
unix 2 [ACC] STREAM LISTENING 14752 /run/lvm/lvmpolld.socket
unix 2 [ACC] STREAM LISTENING 14757 /run/rpcbind.sock
unix 2 [ACC] STREAM LISTENING 23559 @ISCSIADM_ABSTRACT_NAMESPACE
unix 2 [ACC] STREAM LISTENING 22209 /var/run/mcelog-client
unix 2 [ACC] STREAM LISTENING 23826 /var/lib/sss/pipes/private/sbus-monitor
unix 2 [ACC] STREAM LISTENING 24077 /var/lib/sss/pipes/nss
unix 2 [ACC] STREAM LISTENING 17405 /var/run/.heim_org.h5l.kcm-socket
[root@c7-2 ~]#
Right Ctrl

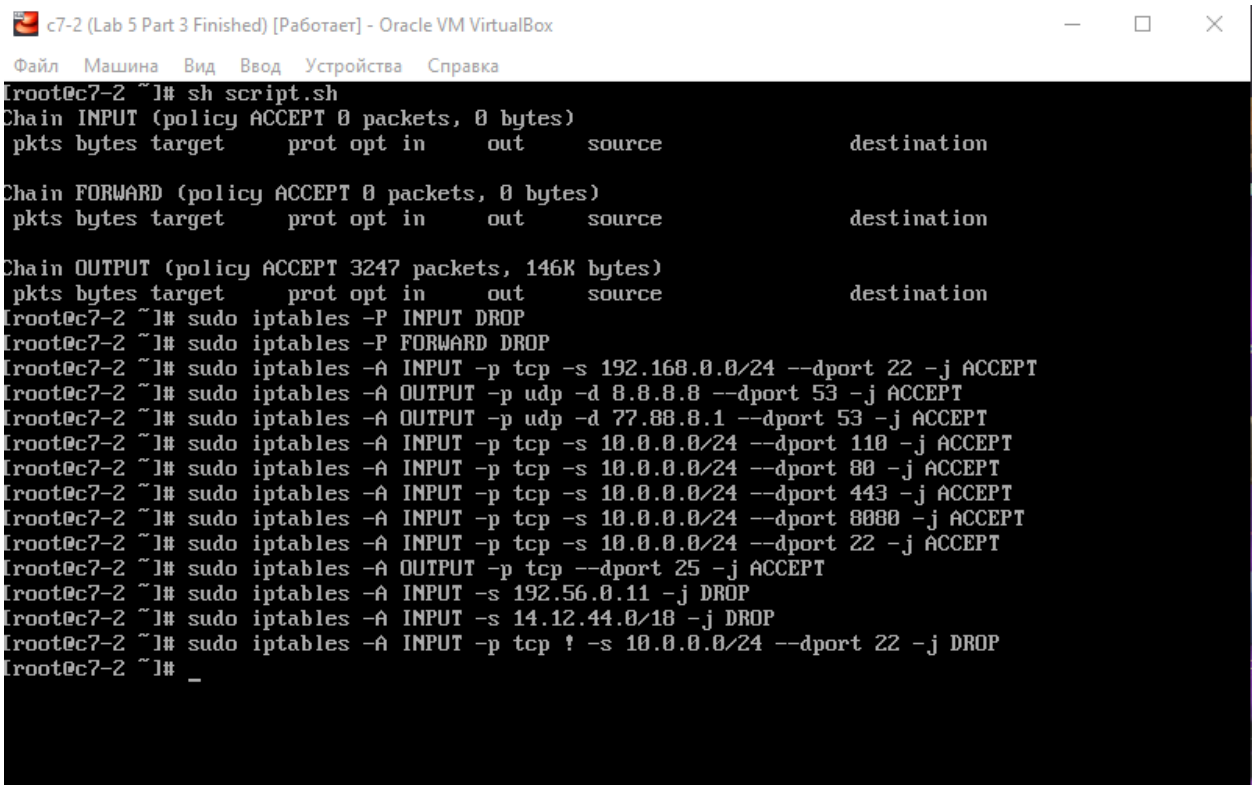

c7-2 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
[root@c7-2 ~]# lsof -i TCP
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
systemd 1 root 38u IPv4 14760 0t0 TCP *:sunrpc (LISTEN)
systemd 1 root 40u IPv6 14762 0t0 TCP *:sunrpc (LISTEN)
rpcbind 849 rpc 4u IPv4 14760 0t0 TCP *:sunrpc (LISTEN)
rpcbind 849 rpc 6u IPv6 14762 0t0 TCP *:sunrpc (LISTEN)
sshd 957 root 4u IPv4 18233 0t0 TCP *:ssh (LISTEN)
sshd 957 root 6u IPv6 18235 0t0 TCP *:ssh (LISTEN)
lighttpd 965 lighttpd 4u IPv4 24067 0t0 TCP *:http (LISTEN)
[root@c7-2 ~]#


c7-1 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
15:37:46.780862 IP (tos 0x0, ttl 2, id 54943, offset 0, flags [DF], proto TCP (6), length 40)
c7-1.33012 > ya.ru.http: Flags [.], cksum 0xbda5 (correct), ack 1, win 29200, length 0
15:37:46.780903 IP (tos 0x0, ttl 2, id 54944, offset 0, flags [DF], proto TCP (6), length 40)
c7-1.33012 > ya.ru.http: Flags [F.], cksum 0xbda4 (correct), seq 1, ack 1, win 29200, length 0
15:37:46.780958 IP (tos 0x0, ttl 64, id 40, offset 0, flags [none], proto TCP (6), length 40)
ya.ru.http > c7-1.33012: Flags [.], cksum 0x2fb5 (correct), ack 2, win 65535, length 0
15:37:46.798791 IP (tos 0x0, ttl 64, id 41, offset 0, flags [none], proto TCP (6), length 40)
ya.ru.http > c7-1.33012: Flags [F.], cksum 0x2fb4 (correct), seq 1, ack 2, win 65535, length 0
15:37:46.798936 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF], proto TCP (6), length 40)
c7-1.33012 > ya.ru.http: Flags [.], cksum 0xbda3 (correct), ack 2, win 29200, length 0
15:37:47.430433 IP (tos 0x0, ttl 1, id 32973, offset 0, flags [DF], proto TCP (6), length 60)
c7-1.33014 > ya.ru.http: Flags [S], cksum 0x7ab4 (correct), seq 1496480210, win 29200, options [
mss 1460,sackOK,TS val 3047721023 ecr 0,nop,wscale 7], length 0
15:37:47.430481 IP (tos 0xc0, ttl 255, id 42, offset 0, flags [none], proto ICMP (1), length 56)
_gateway > c7-1: ICMP time exceeded in-transit, length 36
IP (tos 0x0, ttl 1, id 32973, offset 0, flags [DF], proto TCP (6), length 60)
c7-1.33014 > ya.ru.http: [|tcp]
15:37:47.764393 IP (tos 0x0, ttl 2, id 43341, offset 0, flags [DF], proto TCP (6), length 60)
c7-1.33015 > ya.ru.http: Flags [S], cksum 0x1baa (correct), seq 2004334920, win 29200, options [
mss 1460,sackOK,TS val 3047721357 ecr 0,nop,wscale 7], length 0
15:37:47.782225 IP (tos 0x0, ttl 64, id 43, offset 0, flags [none], proto TCP (6), length 44)
ya.ru.http > c7-1.33015: Flags [S.], cksum 0x5b71 (correct), seq 54720001, ack 2004334921, win 6
5535, options [mss 1460], length 0
15:37:47.782375 IP (tos 0x0, ttl 2, id 43342, offset 0, flags [DF], proto TCP (6), length 40)
c7-1.33015 > ya.ru.http: Flags [.], cksum 0x011e (correct), ack 1, win 29200, length 0
15:37:47.782383 IP (tos 0x0, ttl 2, id 43343, offset 0, flags [DF], proto TCP (6), length 40)
c7-1.33015 > ya.ru.http: Flags [F.], cksum 0x011d (correct), seq 1, ack 1, win 29200, length 0
15:37:47.782434 IP (tos 0x0, ttl 64, id 44, offset 0, flags [none], proto TCP (6), length 40)
ya.ru.http > c7-1.33015: Flags [.], cksum 0x732d (correct), ack 2, win 65535, length 0
15:37:47.799850 IP (tos 0x0, ttl 64, id 45, offset 0, flags [none], proto TCP (6), length 40)
ya.ru.http > c7-1.33015: Flags [F.], cksum 0x732c (correct), seq 1, ack 2, win 65535, length 0
15:37:47.800022 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF], proto TCP (6), length 40)
c7-1.33015 > ya.ru.http: Flags [.], cksum 0x011c (correct), ack 2, win 29200, length 0
15:37:48.441876 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has _gateway tell c7-1, length 28
15:37:48.441958 ARP, Ethernet (len 6), IPv4 (len 4), Reply _gateway is-at 52:54:00:12:35:02 (oui Unk
nown), length 46
Right Ctrl
c7-2 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
My traceroute [v0.92]
c7-2 (10.0.0.2) 2023-04-11T15:37:53+0300
Keys: Help Display mode Restart statistics Order of fields quit
Packets Pings
Host Loss% Snt Last Avg Best Wrst StDev
1. _gateway 0.0% 5 0.2 0.2 0.2 0.4 0.1
2. 10.0.2.2 0.0% 5 0.3 0.2 0.2 0.3 0.0
3. ya.ru 0.0% 5 18.1 18.1 17.2 18.4 0.5
[root@c7-2 ~]# _
Right Ctrl


c7-1 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
YSNuser@c7-2:~
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
C:\Users\csgod>ssh YSNuser@127.0.0.1 -p 55022
YSNuser@127.0.0.1's password:
Activate the web console with: systemctl enable --now cockpit.socket
Last login: Mon Apr 10 18:24:33 2023 from 10.0.2.2
YSNuser@c7-2 ~]$
Right Ctrl
c7-2 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
15:40:10.420562 IP (tos 0x0, ttl 63, id 66, offset 0, flags [none], proto TCP (6), length 40)
10.0.2.2.60892 > c7-2.ssh: Flags [.], cksum 0xbf57 (correct), seq 1862, ack 2350, win 65535, len
gth 0
15:40:10.420636 IP (tos 0x0, ttl 63, id 67, offset 0, flags [none], proto TCP (6), length 176)
10.0.2.2.60892 > c7-2.ssh: Flags [P.], cksum 0xe992 (correct), seq 1862:1998, ack 2350, win 6553
5, length 136
15:40:10.420642 IP (tos 0x0, ttl 64, id 32716, offset 0, flags [DF], proto TCP (6), length 40)
c7-2.ssh > 10.0.2.2.60892: Flags [.], cksum 0x161e (incorrect -> 0x2bff), seq 2350, ack 1998, wi
n 37504, length 0
15:40:10.422455 IP (tos 0x40, ttl 64, id 32717, offset 0, flags [DF], proto TCP (6), length 148)
c7-2.ssh > 10.0.2.2.60892: Flags [P.], cksum 0x168a (incorrect -> 0xcf66), seq 2350:2458, ack 19
98, win 37504, length 108
15:40:10.422605 IP (tos 0x0, ttl 63, id 68, offset 0, flags [none], proto TCP (6), length 40)
10.0.2.2.60892 > c7-2.ssh: Flags [.], cksum 0xbe63 (correct), seq 1998, ack 2458, win 65535, len
gth 0
15:40:10.423894 IP (tos 0x40, ttl 64, id 32718, offset 0, flags [DF], proto TCP (6), length 204)
c7-2.ssh > 10.0.2.2.60892: Flags [P.], cksum 0x16c2 (incorrect -> 0x8128), seq 2458:2622, ack 19
98, win 37504, length 164
15:40:10.424067 IP (tos 0x0, ttl 63, id 69, offset 0, flags [none], proto TCP (6), length 40)
10.0.2.2.60892 > c7-2.ssh: Flags [.], cksum 0xbdbf (correct), seq 1998, ack 2622, win 65535, len
gth 0
15:40:10.454027 IP (tos 0x40, ttl 64, id 32719, offset 0, flags [DF], proto TCP (6), length 116)
c7-2.ssh > 10.0.2.2.60892: Flags [P.], cksum 0x166a (incorrect -> 0xbebf), seq 2622:2698, ack 19
98, win 37504, length 76
15:40:10.454263 IP (tos 0x0, ttl 63, id 70, offset 0, flags [none], proto TCP (6), length 40)
10.0.2.2.60892 > c7-2.ssh: Flags [.], cksum 0xbd73 (correct), seq 1998, ack 2698, win 65535, len
gth 0
15:40:12.320424 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has c7-2 tell _gateway, length 46
15:40:12.320432 ARP, Ethernet (len 6), IPv4 (len 4), Reply c7-2 is-at 08:00:27:36:ee:e7 (oui Unknown
), length 28
15:40:12.320554 IP (tos 0x0, ttl 64, id 37903, offset 0, flags [DF], proto UDP (17), length 67)
c7-2.58799 > dns.google.domain: [bad udp cksum 0x1a52 -> 0x3886!] 17597+ PTR? 1.0.0.10.in-addr.a
rpa. (39)
15:40:12.327053 IP (tos 0x0, ttl 63, id 71, offset 0, flags [none], proto UDP (17), length 67)
dns.google.domain > c7-2.58799: [udp sum ok] 17597 NXDomain q: PTR? 1.0.0.10.in-addr.arpa. 0/0/0
(39)
Right Ctrl

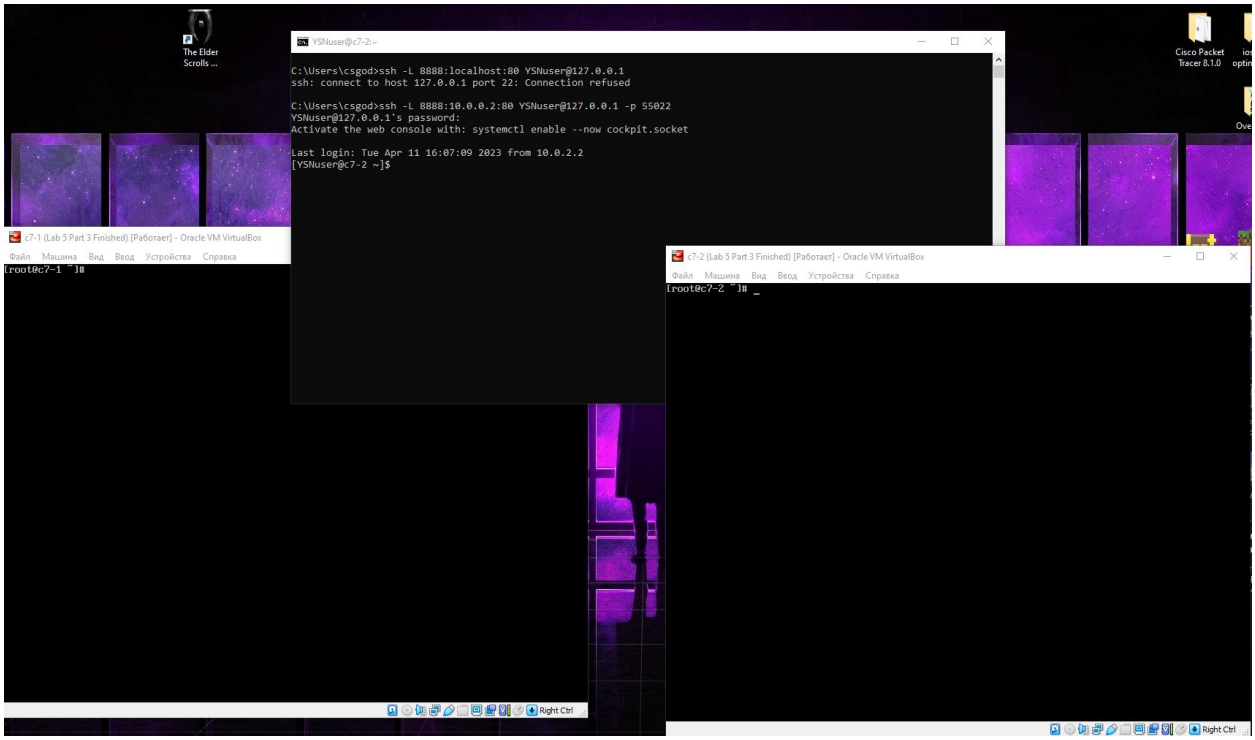

c7-2 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
root@c7-2 ~]# tcpdump -i enp0s3 -vvv
542.425137] device enp0s3 entered promiscuous mode
dropped privs to tcpdump
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
15:40:07.241656 IP (tos 0x0, ttl 63, id 46, offset 0, flags [none], proto TCP (6), length 44)
10.0.2.2.60892 > c7-2.ssh: Flags [S], cksum 0x29db (correct), seq 72640001, win 65535, options [
mss 1460], length 0
15:40:07.241688 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 44)
c7-2.ssh > 10.0.2.2.60892: Flags [S.], cksum 0x1622 (incorrect -> 0x45fc), seq 1321476857, ack 7
2640002, win 29200, options [mss 1460], length 0
15:40:07.241829 IP (tos 0x0, ttl 63, id 47, offset 0, flags [none], proto TCP (6), length 40)
10.0.2.2.60892 > c7-2.ssh: Flags [.], cksum 0xcfc9 (correct), seq 1, ack 1, win 65535, length 0
15:40:07.242166 IP (tos 0x0, ttl 64, id 35994, offset 0, flags [DF], proto UDP (17), length 67)
c7-2.48608 > dns.google.domain: [bad udp cksum 0x1a52 -> 0x000e!] 42115+ PTR? 2.0.0.10.in-addr.a
rpa. (39)
15:40:07.242778 IP (tos 0x0, ttl 63, id 48, offset 0, flags [none], proto TCP (6), length 73)
10.0.2.2.60892 > c7-2.ssh: Flags [P.], cksum 0x8c84 (correct), seq 1:34, ack 1, win 65535, lengt
h 33
15:40:07.242786 IP (tos 0x0, ttl 64, id 32704, offset 0, flags [DF], proto TCP (6), length 40)
c7-2.ssh > 10.0.2.2.60892: Flags [.], cksum 0x161e (incorrect -> 0x5d98), seq 1, ack 34, win 292
00, length 0
15:40:07.247581 IP (tos 0x0, ttl 64, id 32705, offset 0, flags [DF], proto TCP (6), length 61)
c7-2.ssh > 10.0.2.2.60892: Flags [P.], cksum 0x1633 (incorrect -> 0x9cd2), seq 1:22, ack 34, win
29200, length 21
15:40:07.247756 IP (tos 0x0, ttl 63, id 49, offset 0, flags [none], proto TCP (6), length 40)
10.0.2.2.60892 > c7-2.ssh: Flags [.], cksum 0xcf93 (correct), seq 34, ack 22, win 65535, length
0
15:40:07.248794 IP (tos 0x0, ttl 63, id 50, offset 0, flags [none], proto UDP (17), length 67)
dns.google.domain > c7-2.48608: [udp sum ok] 42115 NXDomain q: PTR? 2.0.0.10.in-addr.arpa. 0/0/0
(39)
15:40:07.249103 IP (tos 0x0, ttl 64, id 36000, offset 0, flags [DF], proto UDP (17), length 67)
c7-2.58688 > dns.google.domain: [bad udp cksum 0x1a52 -> 0xbf0a!] 48676+ PTR? 2.2.0.10.in-addr.a
rpa. (39)
15:40:07.250698 IP (tos 0x0, ttl 64, id 32706, offset 0, flags [DF], proto TCP (6), length 1088)
c7-2.ssh > 10.0.2.2.60892: Flags [P.], cksum 0x1a36 (incorrect -> 0xdaf2), seq 22:1070, ack 34,
win 29200, length 1048
15:40:07.250844 IP (tos 0x0, ttl 63, id 51, offset 0, flags [none], proto TCP (6), length 40)
Right Ctrl

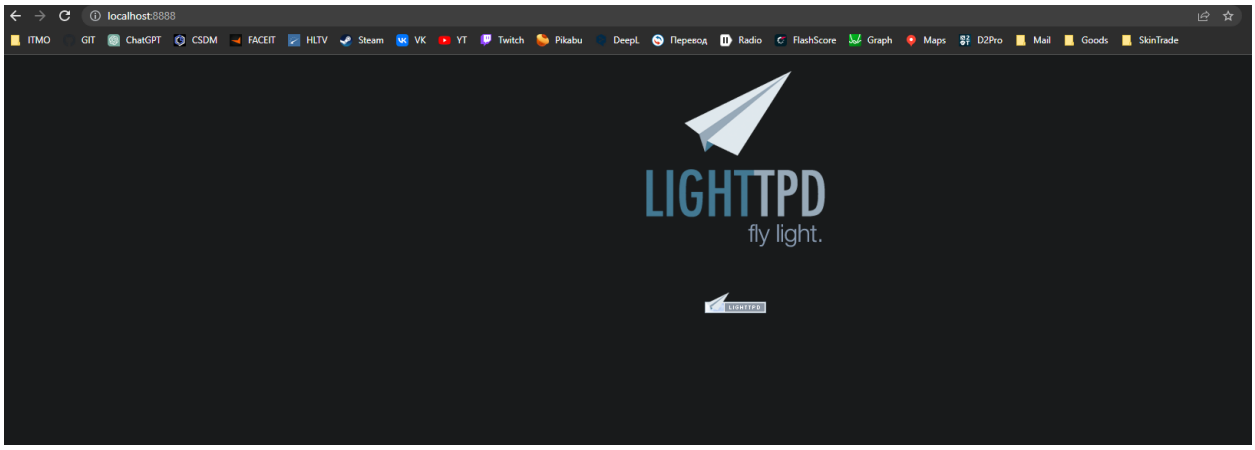
Часть 6:


c7-2 (Lab 5 Part 3 Finished) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
[root@c7-2 ~]# sh script.sh
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 3247 packets, 146K bytes)
pkts bytes target prot opt in out source destination
[root@c7-2 ~]# sudo iptables -P INPUT DROP
[root@c7-2 ~]# sudo iptables -P FORWARD DROP
[root@c7-2 ~]# sudo iptables -A INPUT -p tcp -s 192.168.0.0/24 --dport 22 -j ACCEPT
[root@c7-2 ~]# sudo iptables -A OUTPUT -p udp -d 8.8.8.8 --dport 53 -j ACCEPT
[root@c7-2 ~]# sudo iptables -A OUTPUT -p udp -d 77.88.8.1 --dport 53 -j ACCEPT
[root@c7-2 ~]# sudo iptables -A INPUT -p tcp -s 10.0.0.0/24 --dport 110 -j ACCEPT
[root@c7-2 ~]# sudo iptables -A INPUT -p tcp -s 10.0.0.0/24 --dport 80 -j ACCEPT
[root@c7-2 ~]# sudo iptables -A INPUT -p tcp -s 10.0.0.0/24 --dport 443 -j ACCEPT
[root@c7-2 ~]# sudo iptables -A INPUT -p tcp -s 10.0.0.0/24 --dport 8080 -j ACCEPT
[root@c7-2 ~]# sudo iptables -A INPUT -p tcp -s 10.0.0.0/24 --dport 22 -j ACCEPT
[root@c7-2 ~]# sudo iptables -A OUTPUT -p tcp --dport 25 -j ACCEPT
[root@c7-2 ~]# sudo iptables -A INPUT -s 192.56.0.11 -j DROP
[root@c7-2 ~]# sudo iptables -A INPUT -s 14.12.44.0/18 -j DROP
[root@c7-2 ~]# sudo iptables -A INPUT -p tcp ! -s 10.0.0.0/24 --dport 22 -j DROP
[root@c7-2 ~]#

Часть 7:

ssh –L 8888:10.0.0.2:80 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.