Лаборатория работа 7

Расширенные настройки межсетевого экрана

ПОДГОТОВИЛА: КИМ РЕАЧНА
ГРУППА: НПИБД-02-20

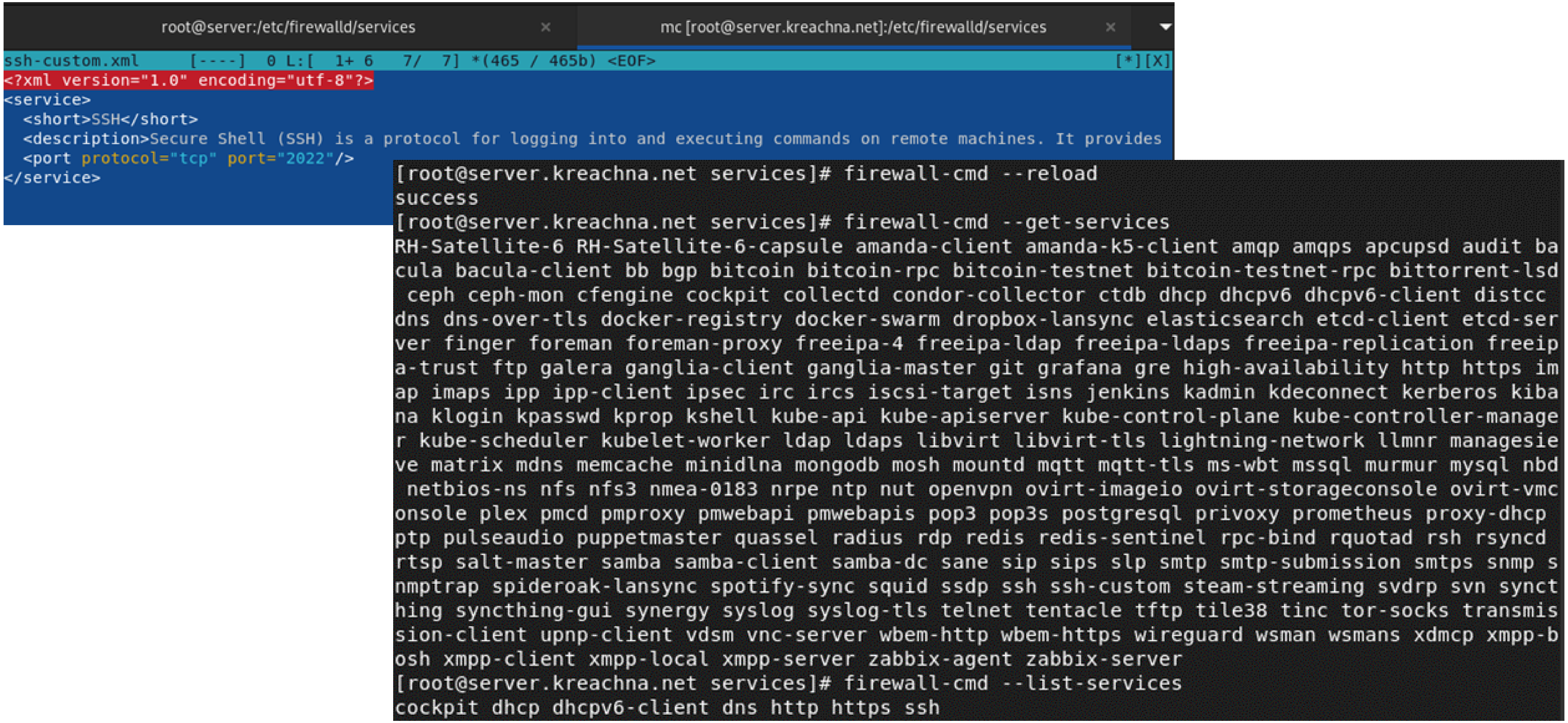
Цель работы:

Получить навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Задание:

- Создание пользовательской службы firewalld
- Перенаправление портов
- Настройка Port Forwarding и Masquerading
- Внесение изменений в настройки внутреннего окружения виртуальной машины

Создание пользовательской службы firewalld

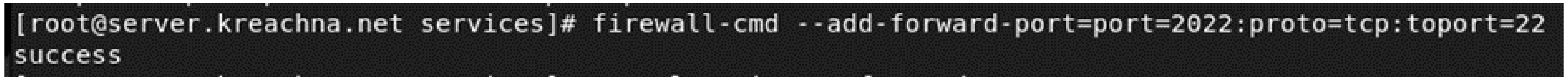


root@server:/etc/firewalld/services
mc [root@server.kreachna.net]:/etc/firewalld/services

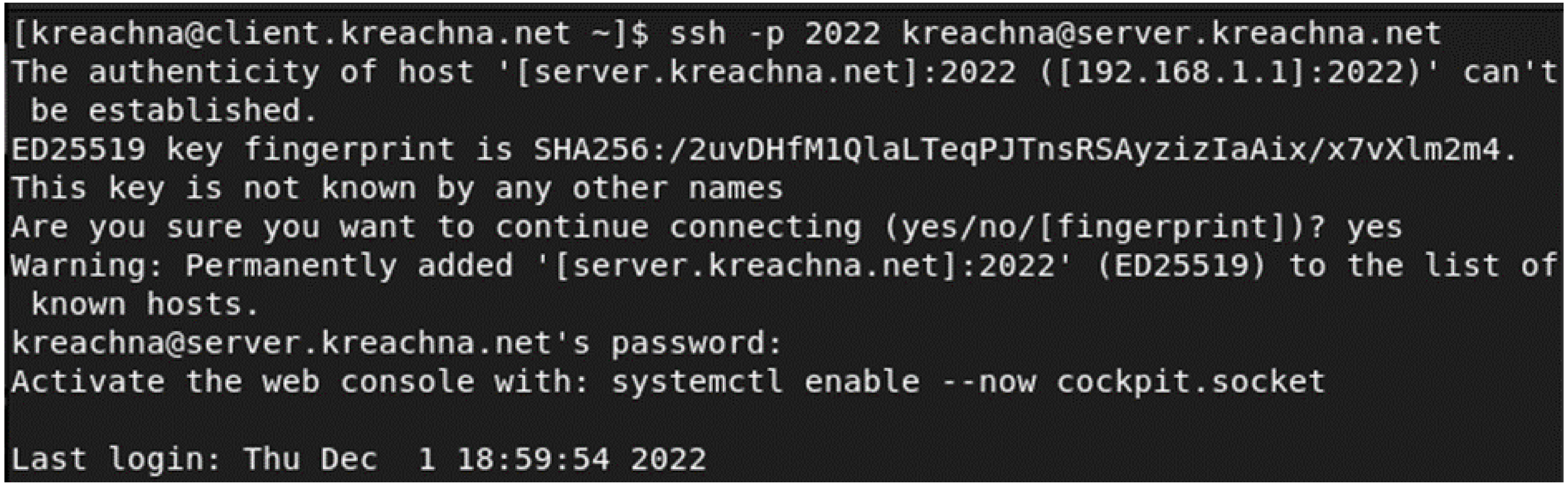
```
ssh-custom.xml     [----]  0 L:[  1+ 6   7/  7] *(465 / 465b) <EOF>                                    [*][X]
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides
  <port protocol="tcp" port="2022"/>
</service>
```

```
[root@server.kreachna.net services]# firewall-cmd --reload
success
[root@server.kreachna.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audit ba
cula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd
 ceph ceph-mon cfengine cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6-client distcc
dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-ser
ver finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeip
a-trust ftp galera ganglia-client ganglia-master git grafana gre high-availability http https im
ap imaps ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kiba
na klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-controller-manage
r kube-scheduler kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr managesie
ve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd
 netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmc
onsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp
ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd
rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp s
nmptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn synct
hing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmis
sion-client upnp-client vdsm vnc-server wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-b
osh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
[root@server.kreachna.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
```

Перенаправление портов



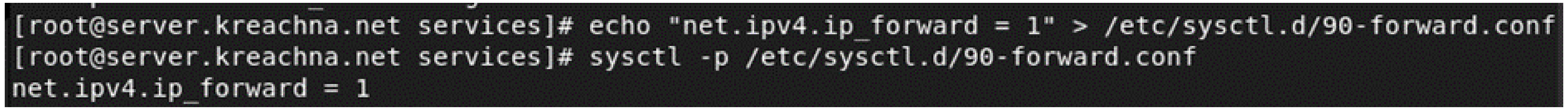
```
[root@server.kreachna.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
```



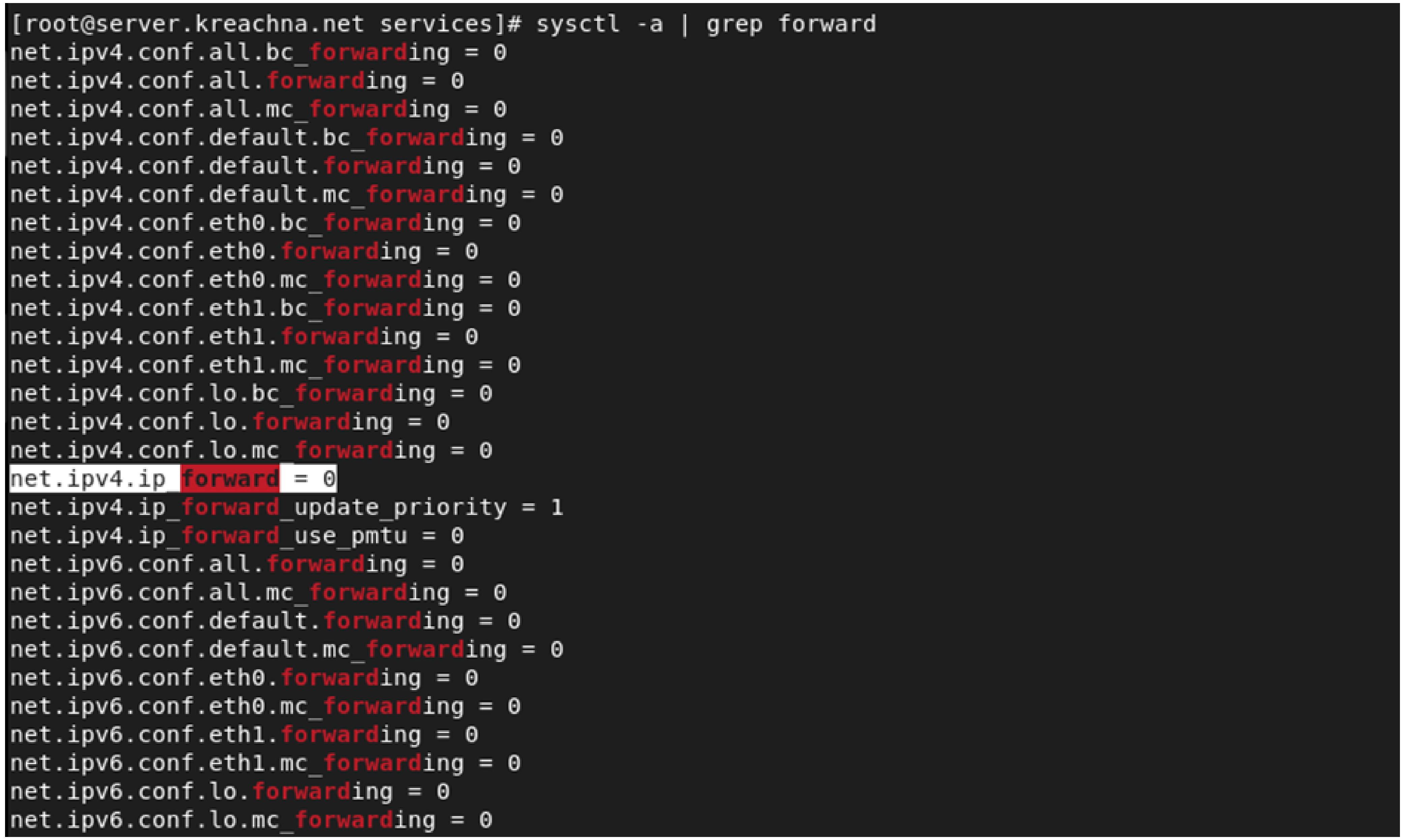
```
[kreachna@client.kreachna.net ~]$ ssh -p 2022 kreachna@server.kreachna.net
The authenticity of host '[server.kreachna.net]:2022 ([192.168.1.1]:2022)' can't
 be established.
ED25519 key fingerprint is SHA256:/2uvDHfM1QlaLTeqPJTnsRSAyzizIaAix/x7vXlm2m4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[server.kreachna.net]:2022' (ED25519) to the list of
 known hosts.
kreachna@server.kreachna.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Thu Dec  1 18:59:54 2022
```

Настройка Port Forwarding и Masquerading

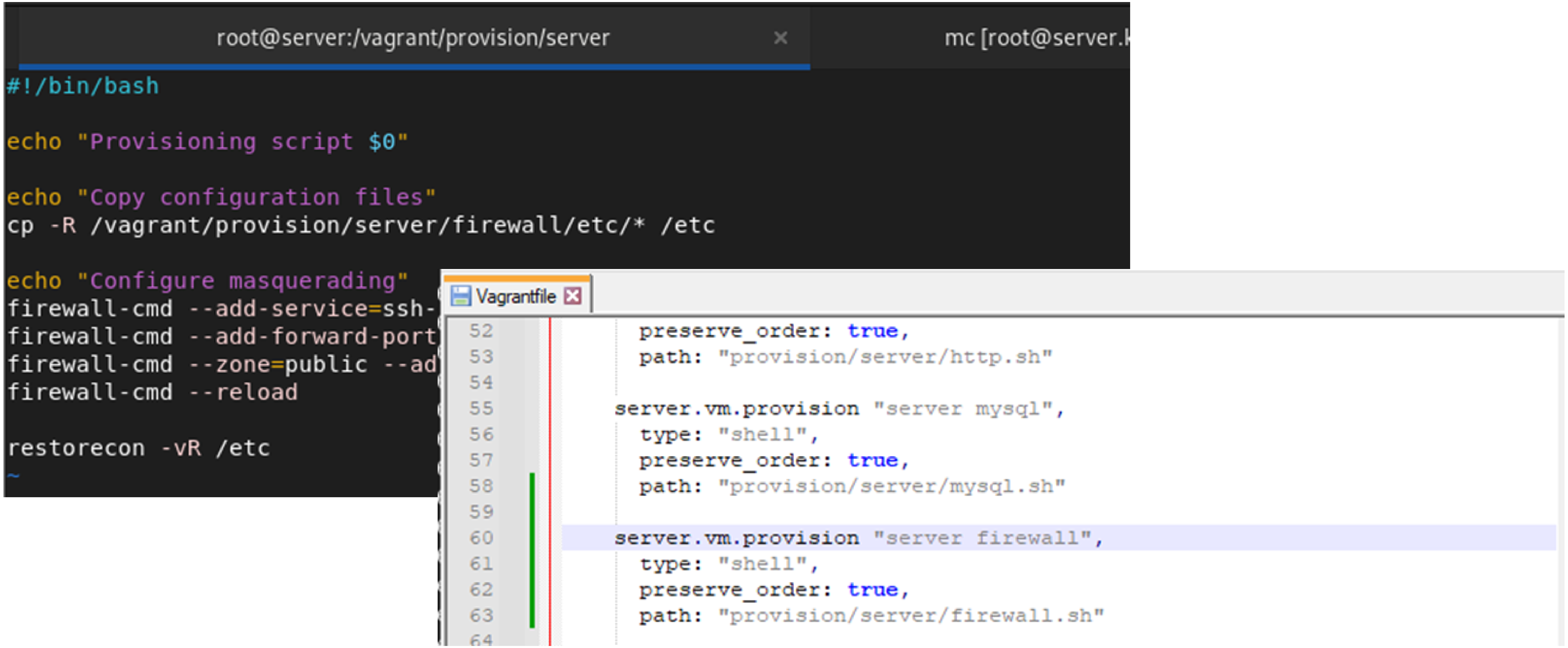


```
[root@server.kreachna.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.kreachna.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
```



```
[root@server.kreachna.net services]# sysctl -a | grep forward
net.ipv4.conf.all.bc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.default.bc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.eth0.bc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth1.bc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.lo.bc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.ip_forward = 0
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.default.mc_forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth0.mc_forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth1.mc_forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv6.conf.lo.mc_forwarding = 0
```

Внесение изменений в настройки внутреннего окружения виртуальной машины



```
#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/firewall/etc/* /etc

echo "Configure masquerading"
firewall-cmd --add-service=ssh-
firewall-cmd --add-forward-port
firewall-cmd --zone=public --ad
firewall-cmd --reload

restorecon -vR /etc
~
```

```
      preserve_order: true,
      path: "provision/server/http.sh"

    server.vm.provision "server mysql",
      type: "shell",
      preserve_order: true,
      path: "provision/server/mysql.sh"

    server.vm.provision "server firewall",
      type: "shell",
      preserve_order: true,
      path: "provision/server/firewall.sh"
```

Вывод

Получила навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Спасибо за внимание!