

Лабораторная работа №7

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

2026-02-13

Содержание I

1 1. Цель работы

2 2. Выполнение лабораторной работы

3 3. Выводы

Раздел 1

1. Цель работы

1.1 Цель работы

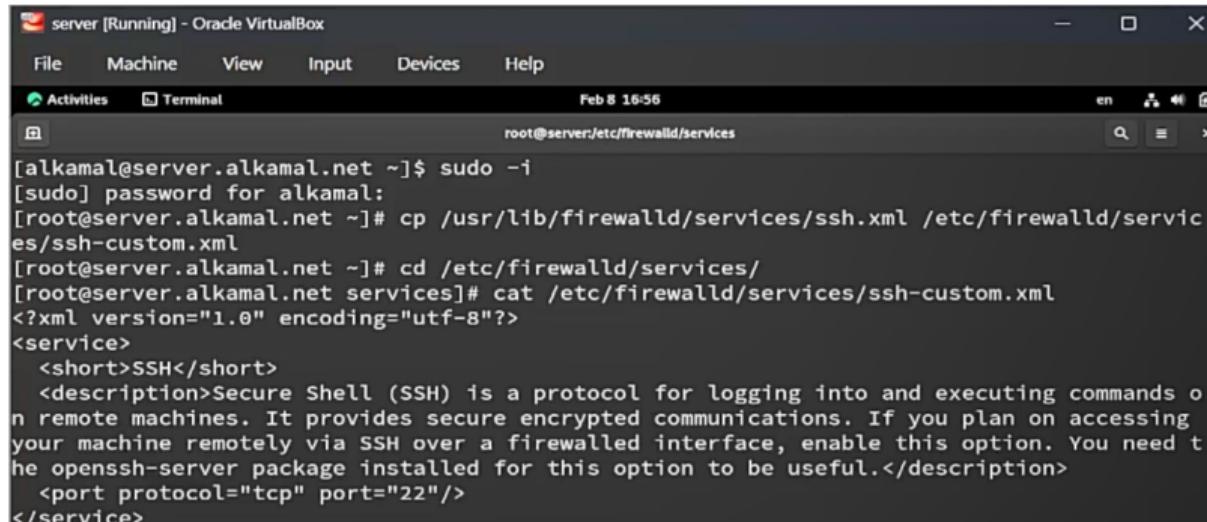
- Получение навыков настройки межсетевого экрана в Linux
- Реализация переадресации портов
- Настройка Masquerading

Раздел 2

2. Выполнение лабораторной работы

2.1 Создание пользовательской службы firewalld

- Выполнен переход в режим суперпользователя
- Скопирован файл ssh.xml в ssh-custom.xml
- Файл размещён в /etc/firewalld/services/



```
[alkamal@server.alkamal.net ~]$ sudo -i
[sudo] password for alkamal:
[root@server.alkamal.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.alkamal.net ~]# cd /etc/firewalld/services/
[root@server.alkamal.net services]# cat /etc/firewalld/services/ssh-custom.xml
<?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 secure encrypted communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the openssh-server package installed for this option to be useful.</description>
    <port protocol="tcp" port="22"/>
</service>
```

Рисунок 1: Копирование файла службы ssh.xml в ssh-custom.xml

- В файле изменён порт с 22 на 2022
- Обновлено описание службы
- Проверено содержимое файла

```
[root@server.alkamal.net services]# nano /etc/firewalld/services/ssh-custom.xml
[root@server.alkamal.net services]# cat /etc/firewalld/services/ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
    <short>SSH</short>
    <description>Модифицированная служба SSH для доступа через порт TCP 2022 (лабораторная
работа №7)</description>
    <port protocol="tcp" port="2022"/>
</service>
```

Рисунок 2: Редактирование службы: изменение порта на 2022 и обновление описания

- Получен список служб --get-services
- Выполнена перезагрузка firewall-cmd --reload
- Служба ssh-custom добавлена в активные
- Добавлена в постоянную конфигурацию

```
[root@server.alkamal.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcup
sd audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storag
e bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph
-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb
dds dds-multicast dds-unicast dhcpc dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-re
gistry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman
foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp
galera ganglia-client ganglia-master git gpgsql grafana gre high-availability http http3 ht
tps ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin
kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-contr
ol-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure
kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-
readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-clie
nt llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt
mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea
-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconso
le plex pmcd pmproxy pmwebapis pmwebapis pop3 pop3s postgresql privoxy prometheus promethe
us-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius
rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-c
lient samba-dc sane sip sips slp smtp smtp-submission smtpts snmp snmpd snmpd-snmptrap snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing s
yncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc t
or-socks transmission-client upnp-client vdsm vnc-server warpinator wbem-http wbem-https
wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans
xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@server.alkamal.net services]# firewall-cmd --reload
success
```



```
success
[root@server.alkamal.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcup
sd audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storag
e bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph
-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb
dds dds-multicast dds-unicast dhcpc dhcpcv6 dhcpcv6-client distcc dns dns-over-tls docker-re
gistry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman
foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp
galera ganglia-client ganglia-master git gpgsql grafana gre high-availability http https ht
tps ident imap imaps ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin
kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-contr
ol-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure
kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-
readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-clie
nt llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt
mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea
-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconso
le plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus promethe
us-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius
rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-c
lient samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmp tls snmp tls-trap snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn
syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp ti
le38 tinc tor-socks transmission-client upnp-client vdsm vnc-server warpinator wbem-https
wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp w
sman wsmans xmpp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
zerotier
[root@server.alkamal.net services]# firewall-cmd --list-services
cockpit dhcp dhcpcv6-client dns http https ssh
[root@server.alkamal.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.alkamal.net services]# firewall-cmd --list-services
cockpit dhcp dhcpcv6-client dns http https ssh ssh-custom
[root@server.alkamal.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.alkamal.net services]# firewall-cmd --reload
success
```



2.2 Перенаправление портов

- Настроено правило перенаправления:
- 2022 → 22 (TCP)
- Правило добавлено в текущую конфигурацию

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

Рисунок 5: Настройка перенаправления порта 2022 на 22 в firewalld

- С клиента выполнено подключение:
- ssh -p 2022 alkamal@server.alkamal.net
- Подтверждена успешная авторизация
- Проверена работа перенаправления

```
[alkamal@client.alkamal.net ~]$ ssh -p 2022 alkamal@server.alkamal.net
The authenticity of host '[server.alkamal.net]:2022 ([192.168.1.1]:2022)' can't be established.
ED25519 key fingerprint is SHA256:tyZwLcMbotNmqKfQJnF9uqdkqiWDcCt9yTQ/dAsIjkS.
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.alkamal.net]:2022' (ED25519) to the list of known hosts.
alkamal@server.alkamal.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Feb  8 16:48:45 2026
[alkamal@server.alkamal.net ~]$
```

Рисунок 6: Подключение по SSH к серверу через порт 2022 с клиента

- Проверен параметр `net.ipv4.ip_forward`
- Значение – 0 (маршрутизация отключена)

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



- Создан файл /etc/sysctl.d/90-forward.conf
- Установлено net.ipv4.ip_forward = 1
- Применена конфигурация sysctl -p
- Включён masquerade в зоне public
- Выполнен firewall-cmd --reload

```
[root@server.alkamal.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
```



- С клиента выполнены ping 8.8.8.8 и ping google.com
- Потерь пакетов нет
- Подтверждён выход в Интернет через сервер

```

client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 8 17:19
alkamal@client:~ alkamal@server:~ alkamal@client:~ 
[alkamal@client.alkamal.net ~]$ 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=254 time=2.19 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=254 time=1.27 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=254 time=0.947 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=254 time=1.30 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=254 time=0.506 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=254 time=1.44 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=254 time=0.578 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6036ms
rtt min/avg/max/mdev = 0.506/1.175/2.190/0.531 ms
[alkamal@client.alkamal.net ~]$ ping google.com
PING google.com (64.233.162.138) 56(84) bytes of data.
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=1 ttl=254 time=2.57 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=2 ttl=254 time=1.37 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=3 ttl=254 time=0.877 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=4 ttl=254 time=1.11 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=5 ttl=254 time=0.821 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=6 ttl=254 time=2.54 ms
^X64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=7 ttl=254 time=0.333 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=8 ttl=254 time=0.839 ms
^C
--- google.com ping statistics ---

```

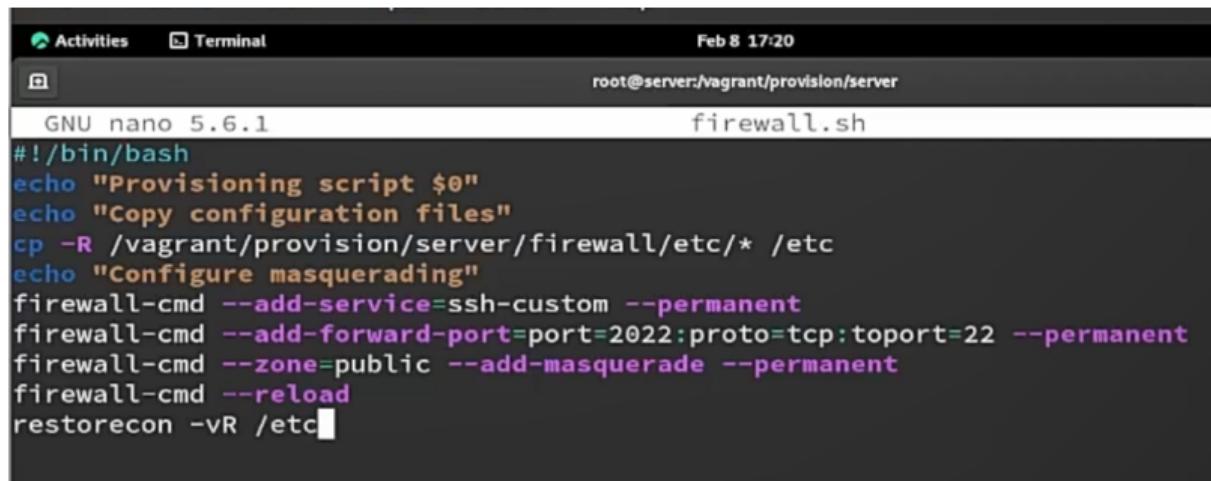
2.3 Внесение изменений в настройки внутреннего

- Созданы каталоги:
- `/etc/firewalld/services`
- `/etc/sysctl.d`
- Скопированы `ssh-custom.xml` и `90-forward.conf`

```
[root@server.alkamal.net services]# cd /vagrant/provision/server
[root@server.alkamal.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.alkamal.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.alkamal.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/services/
[root@server.alkamal.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d/
[root@server.alkamal.net server]# cd /vagrant/provision/server
[root@server.alkamal.net server]# touch firewall.sh
[root@server.alkamal.net server]# chmod +x firewall.sh
[root@server.alkamal.net server]# nano firewall.sh
```

Рисунок 10: Создание структуры каталогов и копирование конфигурационных файлов FirewallD

- Создан скрипт `firewall.sh`
- Реализовано:
 - копирование конфигураций в `/etc`
 - добавление службы `ssh-custom`
 - перенаправление `2022 → 22`
 - включение masquerade
 - перезагрузка `firewalld`
 - восстановление SELinux-контекстов



The screenshot shows a terminal window titled "Terminal" with the command "root@server:/vagrant/provision/server". The window displays the following content:

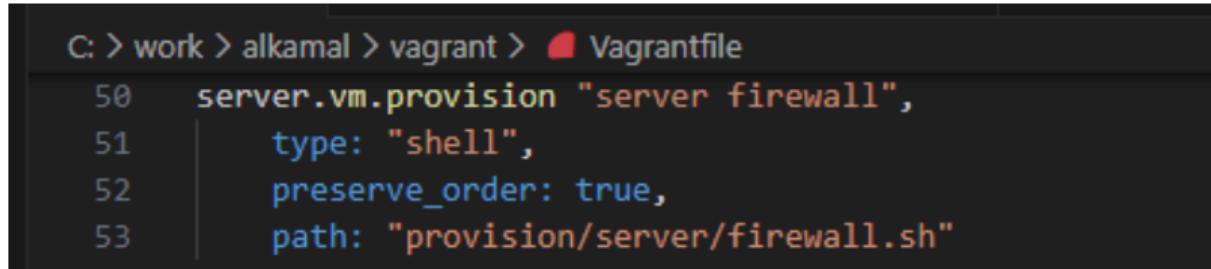
```

GNU nano 5.6.1                               firewall.sh
#!/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-custom --permanent
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22 --permanent
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload
restorecon -vR /etc

```

Рисунок 11: Содержимое provisioning-скрипта `firewall.sh`

- В Vagrantfile добавлен provision-блок
- Тип shell
- Путь provision/server/firewall.sh
- Указан preserve_order: true



```
C: > work > alkamal > vagrant > Vagrantfile
  50   server.vm.provision "server firewall",
  51     type: "shell",
  52     preserve_order: true,
  53     path: "provision/server/firewall.sh"
```

Рисунок 12: Добавление provisioning-скрипта firewall.sh в Vagrantfile

Раздел 3

3. Выводы

3.1 Выводы

- Создана пользовательская служба `ssh-custom` (порт 2022)
- Реализовано перенаправление `2022 → 22`
- Подтверждён SSH-доступ через нестандартный порт
- Включена маршрутизация IPv4 (`ip_forward = 1`)
- Настроен masquerading в зоне `public`
- Подтверждён выход клиента в Интернет через сервер
- Реализована автоматизация через `firewall.sh` и `Vagrantfile`