

Лабораторная работа №7

Администрирование сетевых подсистем

Мишина А. А.

16 октября 2024

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

Выполнение лабораторной работы

Создание пользовательской службы firewalld



```
root@server:/etc/firewalld/services

[aamishina@server.aamishina.net ~]$ sudo -i
[sudo] password for aamishina:
[root@server.aamishina.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.aamishina.net ~]# cd /etc/firewalld/services/
[root@server.aamishina.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>
[root@server.aamishina.net services]#
```

Рис. 1: Создание собственного файла описания службы и просмотр



```
root@server:/etc/firewalld/services

<?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. File was modified.</description>
  <port protocol="tcp" port="22"/>
</service>
~
~
~
~
~
~
```

Рис. 2: Редактирование файла описания службы

Список доступных служб

```
p spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog
syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsman vnc-server warpinator wben-http
wben-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsmann xdmcp xmpp-bosh xmpp-client
xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@server.aamishina.net services]# firewall-cmd --reload
success
[root@server.aamishina.net services]# firewall-cmd --get-services
AH-Satellite-6 AH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-cl
ient bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorren
t-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-
unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-clie
nt etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera
ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ips
irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver ku
be-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-
scheduler kube-scheduler-secure kube-worker kubernetes kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-n
etwork llmr llmr-client llmr-tcp llmr-udp managesieve matrix mdns memcached minidlna mongodb mosh mountr mqt mqt-tls ms-w
bt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-stor
ageconsole ovirt-vmconsole plex pmdc pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-expor
ter proxy-dhcp ps2link ps3netvr ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyn
cd rtsp salt-master samba samba-client samba-dc sane sip sipsec slp smtp smtp-submission snmp snmpd snmpd-trap snmptrap
p spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay s
ynergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsman vnc-server warpinator
wben-http wben-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsmann xdmcp xmpp-bos
h xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@server.aamishina.net services]#
```

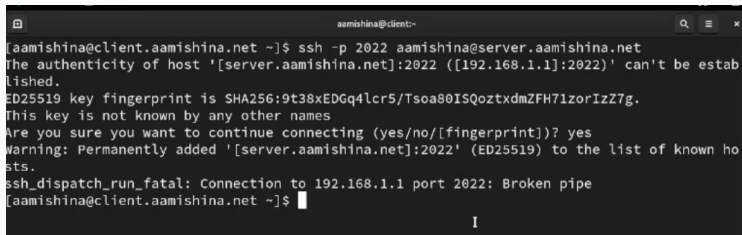
Рис. 3: Перезагрузка правил межсетевого экрана, новая служба

```
[root@server.aamishina.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.aamishina.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.aamishina.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.aamishina.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.aamishina.net services]# firewall-cmd --reload
success
[root@server.aamishina.net services]#
```

Рис. 4: Добавление новой службы в FirewallD и просмотр списка активных служб, сохранение информации о состоянии

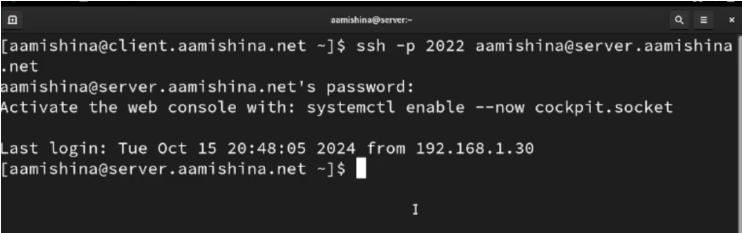
Перенаправление портов

- Переадресация порта: `firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22`

A terminal window titled 'aamishina@client:~' showing an SSH command and its output. The command is 'ssh -p 2022 aamishina@server.aamishina.net'. The output shows a warning about the host's authenticity, a fingerprint, and a confirmation to continue. The connection then fails with a 'Broken pipe' error.

```
aamishina@client:~  
[aamishina@client.aamishina.net ~]$ ssh -p 2022 aamishina@server.aamishina.net  
The authenticity of host '[server.aamishina.net]:2022 ([192.168.1.1]:2022)' can't be estab  
lished.  
ED25519 key fingerprint is SHA256:9t38xEDGq4lcr5/Tsoa80ISQoztxdmZFH71zorIzZ7g.  
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.aamishina.net]:2022' (ED25519) to the list of known ho  
sts.  
ssh_dispatch_run_fatal: Connection to 192.168.1.1 port 2022: Broken pipe  
[aamishina@client.aamishina.net ~]$
```

Рис. 5: Доступ по SSH к серверу через порт 2022 на клиенте

A terminal window titled 'aamishina@server:~' with search, menu, and close icons in the title bar. The terminal shows the execution of an SSH command from a client to a server. The output includes the password prompt, a system message about Cockpit, and the last login information.

```
aamishina@server:~  
[aamishina@client.aamishina.net ~]$ ssh -p 2022 aamishina@server.aamishina.net  
aamishina@server.aamishina.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Tue Oct 15 20:48:05 2024 from 192.168.1.30  
[aamishina@server.aamishina.net ~]$
```

Рис. 6: Доступ по SSH к серверу через порт 2022 на клиенте

Настройка Port Forwarding и Masquerading

```
root@server:~# cat /etc/sysctl.d/90-forward.conf
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.bc_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_mtu = 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:~# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
(root@server:~# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
(root@server:~# firewall-cmd --zone=public --add-masquerade --permanent
success
(root@server:~# firewall-cmd --reload
success
(root@server:~#
```

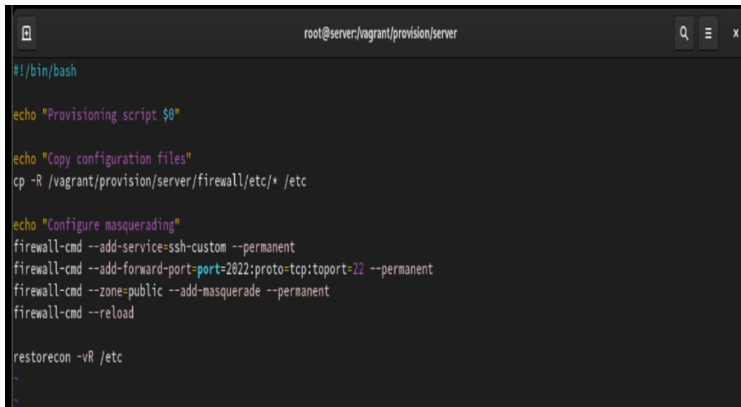
Рис. 7: Включение перенаправления пакетов и включение маскарадинга

Внесение изменений в настройки
внутреннего окружения
виртуальной машины

Внесение изменений в настройки внутреннего окружения

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

Рис. 8: Создание каталогов и копирование конфигурационных файлов, создание скрипта firewall.sh

A terminal window with a dark background and light-colored text. The window title bar shows 'root@server:vagrant/provision/server' and standard window controls (search, menu, close). The terminal content shows a shell prompt followed by several lines of shell script code. The code includes echo statements for logging, a cp command to copy files, another echo statement, firewall-cmd commands to configure services and masquerading, and a restorecon command.

```
#!/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
```

Рис. 9: Редактирование firewall.sh

- В результате выполнения работы были приобретены практические навыки по установке и конфигурированию системы управления базами данных на примере программного обеспечения MariaDB.