

Лабораторная работа №13.

Управление SELinux

Жукова А.А

29 ноября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Жукова Арина Александровна
- Студент бакалавриата, 2 курс
- группа: НПИбд-03-23
- Российский университет дружбы народов
- 1132239120@rudn.ru



Вводная часть

Цель работы

Лабораторная работа направлена на получение навыков настройки пакетного фильтра в Linux.

Задание

1. Используя `firewall-cmd`: – определить текущую зону по умолчанию; – определить доступные для настройки зоны; – определить службы, включённые в текущую зону; – добавить сервер VNC в конфигурацию брандмауэра.
2. Используя `firewall-config`: – добавьте службы `http` и `ssh` в зону `public`; – добавьте порт `2022` протокола `UDP` в зону `public`; – добавьте службу `ftp`.
3. Выполните задание для самостоятельной работы (раздел 13.5).

Результаты и анализ лабораторной работы

Управление брандмауэром с помощью firewall-cmd

1. Определение текущей зоны по умолчанию: `firewall-cmd --get-default-zone`.
2. Определение доступных зон `firewall-cmd --get-zones`.
3. Просмотр служб, доступных на компьютере `firewall-cmd --get-services`.
4. Определение доступных служб в текущей зоне `firewall-cmd --list-services`.

```
[root@aazhukova1 ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@aazhukova1 ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula
bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-tes
tnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb
ctdb dds dds-multicast dds-unicast dhcp dhcpcv6 dhcpcv6-client distcc dns dns-over-tls docker-registry docker-swarm dro
pbox-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 htt
p http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerber
s kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-contro
ller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker k
ubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp
llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd n
ebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-v
mconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy
-dhcp ps2link ps3netsrv 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 sips slp smtp smtp-submission smtps snmp snmpd snmpd-tr
ap snmptrap 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 vdsm vnc-s
erver warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp ws
```

Управление брандмауэром с помощью firewall-cmd

5. Добавление сервера в конфигурацию брандмауэра `firewall-cmd`

```
--add-service=vnc-server.
```

```
[root@aazhukoval ~]# firewall-cmd --add-service=vnc-server
success
[root@aazhukoval ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
```

Управление брандмауэром с помощью firewall-cmd

6. Перезапуск службы firewalld.

```
[root@aazhukoval ~]# systemctl restart firewalld
[root@aazhukoval ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich_rules:
```

Управление брандмауэром с помощью firewall-cmd

7. Добавление службы как постоянной.

```
[root@aazhukova1 ~]# firewall-cmd --add-service=vnc-server --permanent
success
[root@aazhukova1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Управление брандмауэром с помощью firewall-cmd

8. Добавление в конфигурацию межсетевого экрана порта 2022 протокола TCP.
9. Перезагрузка конфигурации firewalld `firewall-cmd --reload`.

```
[root@aazhukova1 ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@aazhukova1 ~]# firewall-cmd --reload
success
[root@aazhukova1 ~]# firewall-cmd --reload
success
[root@aazhukova1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-nat:
  icmp-blocks:
  rich规则:
```

Управление брандмауэром с помощью firewall-config

1. Включение служб.

Firewall Configuration

File Options View Help

Active Bindings

Configuration: Permanent

Connections

- lo (lo)
Default Zone: public
- enp0s3 (enp0s3)
Default Zone: public

enp0s3 (enp0s3)
Default Zone: public

Sources

Zones Services IPSets

A firewalld zone defines the level of trust for network connections, interfaces and source addresses bound to the zone. The zone combines services, ports, protocols, masquerading, port/packet forwarding, icmp filters and rich rules. The zone can be bound to interfaces and source addresses.

block
dmz
drop
external
home
internal
nm-shared
public
trusted
work

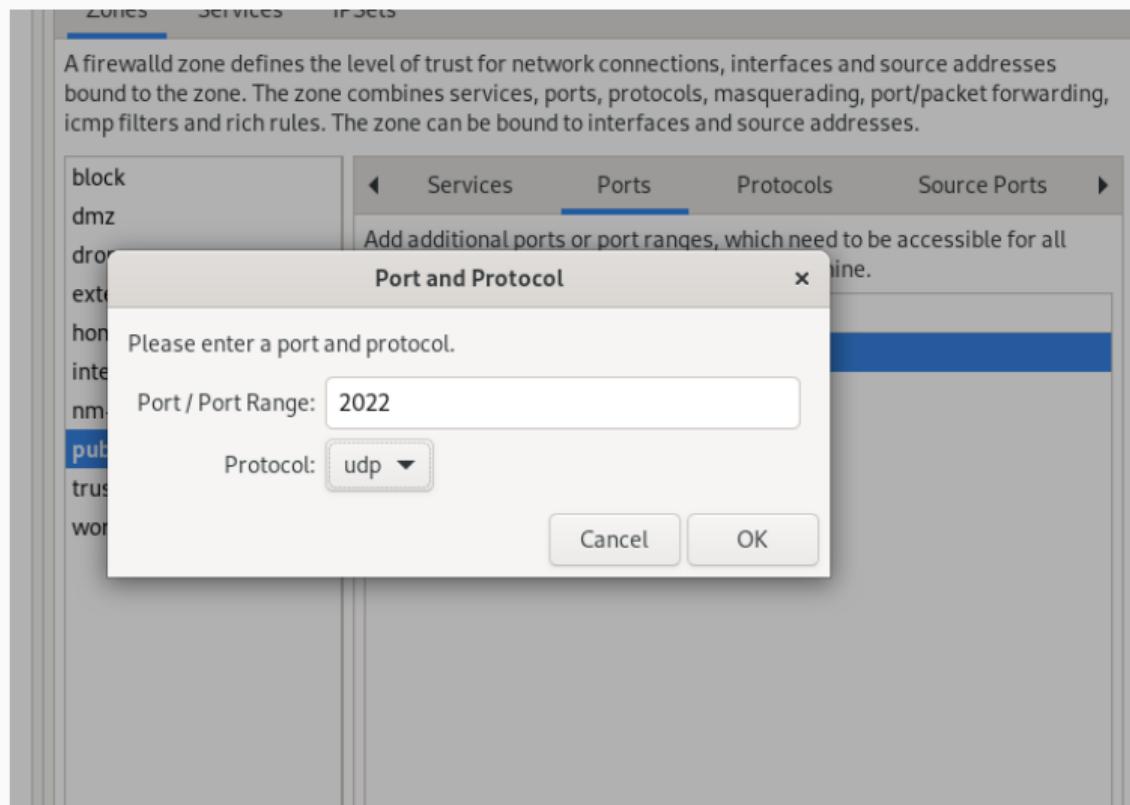
Services Ports Protocols Source Ports

Here you can define which services are trusted in the zone. Trusted services are accessible from all hosts and networks that can reach the machine from connections, interfaces and sources bound to this zone.

| Service |
|--|
| <input type="checkbox"/> freeipa-trust |
| <input checked="" type="checkbox"/> ftp |
| <input type="checkbox"/> galera |
| <input type="checkbox"/> ganglia-client |
| <input type="checkbox"/> ganglia-master |
| <input type="checkbox"/> git |
| <input type="checkbox"/> gpsd |
| <input type="checkbox"/> grafana |
| <input type="checkbox"/> gre |
| <input type="checkbox"/> high-availability |
| <input checked="" type="checkbox"/> http |
| <input type="checkbox"/> http3 |
| <input checked="" type="checkbox"/> https |

Управление брандмауэром с помощью firewall-config

2. Добавление портов.



Выводы

Выводы

В ходе выполнения лабораторной работы были получены навыки настройки пакетного фильтра в Linux.