

ОТЧЕТ ЛАБОРАТОРНОЙ РАБОТЫ 7

ДИСЦИПЛИНА

АДМИНИСТРИРОВАНИЕ СЕТЕВЫХ
ПОДСИСТЕМ

Марина Астахова

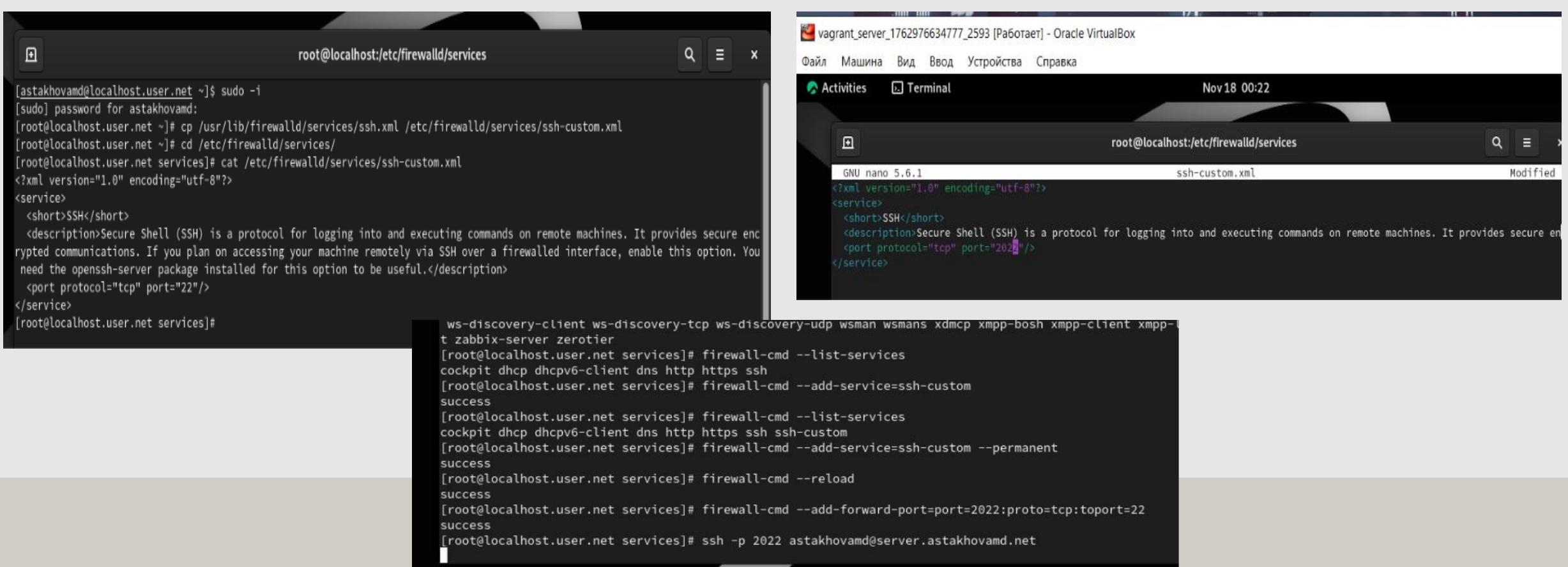
НПИБД-02-23

РАСШИРЕННЫЕ НАСТРОЙКИ МЕЖСЕТЕВОГО ЭКРАНА

Цель работы

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

СОЗДАНИЕ ПОЛЬЗОВАТЕЛЬСКОЙ СЛУЖБЫ FIREWALLD



```
[astakhovamd@localhost.user.net ~]$ sudo -i
[sudo] password for astakhovamd:
[root@localhost.user.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@localhost.user.net ~]# cd /etc/firewalld/services/
[root@localhost.user.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@localhost.user.net services]# ws-discovery-client ws-discovery-tcp ws-discovery-udp wsmans xdmcp xmpp-bosh xmpp-client xmpp-listener zabbix-server zerotier
[root@localhost.user.net services]# firewall-cmd --list-services
cockpit dhcp dhcpcv6-client dns http https ssh
[root@localhost.user.net services]# firewall-cmd --add-service=ssh-custom
success
[root@localhost.user.net services]# firewall-cmd --list-services
cockpit dhcp dhcpcv6-client dns http https ssh ssh-custom
[root@localhost.user.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@localhost.user.net services]# firewall-cmd --reload
success
[root@localhost.user.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@localhost.user.net services]# ssh -p 2022 astakhovamd@server.astakhovamd.net
```

```
vagrant_server_1762976634777_2593 [Работает] - Oracle VirtualBox
Файл Машина Вид Ввод Устройства Справка
Activities Terminal Nov 18 00:22
root@localhost:/etc/firewalld/services
GNU nano 5.6.1          ssh-custom.xml      Modified
<?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="2022"/>
</service>
```

НАСТРОЙКА PORT FORWARDING И MASQUERADING.

```
ssh connect to host server.vastanovka.net port 2222 connection refused
[root@localhost.user.net services]# systemctl start sshd
[root@localhost.user.net services]# systemctl enable sshd
[root@localhost.user.net services]#     grep Port /etc/ssh/sshd_config
```

```
#Port 22
#GatewayPorts no
[root@localhost.user.net services]#     systemctl restart sshd

[root@localhost.user.net services]# firewall-cmd --zone=public --add-port=2022/tcp --permanent
success
[root@localhost.user.net services]# firewall-cmd --reload
success
[root@localhost.user.net services]#     ss -tulpen | grep 2022

[root@localhost.user.net services]#
```

```
[root@localhost.user.net services]#     grep Port /etc/ssh/sshd_config
#Port 22
#GatewayPorts no
[root@localhost.user.net services]#     systemctl restart sshd

[root@localhost.user.net services]# firewall-cmd --zone=public --add-port=2022/tcp --permanent
success
[root@localhost.user.net services]# firewall-cmd --reload
success
[root@localhost.user.net services]#     ss -tulpen | grep 2022

[root@localhost.user.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@localhost.user.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@localhost.user.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@localhost.user.net services]# firewall-cmd --reload
success
[root@localhost.user.net services]#
```

```
[root@vagrant-ubuntu-trusty-64:~# cd /vagrant/provision/server
root@vagrant-ubuntu-trusty-64:/vagrant/provision/server# mkdir -p /vagrant/provision/server/firewall
/etc/firewalld/services
root@vagrant-ubuntu-trusty-64:/vagrant/provision/server# mkdir -p /vagrant/provision/server/firewall
/etc/sysctl.d
root@vagrant-ubuntu-trusty-64:/vagrant/provision/server#
```



ВНЕСЕНИЕ ИЗМЕНЕНИЙ В НАСТРОЙКИ ВНУТРЕННЕГО ОКРУЖЕНИЯ ВИРТУАЛЬНОЙ МАШИНЫ

```
root@localhost:/vagrant/provision/server
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
```

```
path: "provision/server/http.sh"
end

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

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

ИТОГ РАБОТЫ

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

СПАСИБО
ЗА ВНИМАНИЕ!
