

# Презентация лабораторной работы №7

Бакулин Никита 1032201747

# Цель работы

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

# Задачи

- Настройте межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022
- Настройте Port Forwarding на виртуальной машине server
- Настройте маскардинг на виртуальной машине server для организации доступа клиента к сети Интернет
- Напишите скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внести изменения в Vagrantfile

# Результаты выполнения

- Настройте межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>[EDITED] Secure Shell (SSH) is a protocol for logging into and ex
ecuting commands on remote machines. It provides secure encrypted communications
. If you plan on accessing your machine remotely via SSH over a firewalled inter
face, enable this option. You need the openssh-server package installed for this
option to be useful.</description>
  <port protocol="tcp" port="2022"/>
</service>
```

Рис. 1

```
p client xmpp local xmpp server zabbix agent zabbix server
[root@server.nabakulin.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.nabakulin.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.nabakulin.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
```

Рис. 2

# Результаты выполнения

- Настройте Port Forwarding на виртуальной машине server

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

Рис. 3

```
[nabakulin@client.nabakulin.net ~]$ ssh -p 2022 nabakulin@server.nabakulin.net  
The authenticity of host '[server.nabakulin.net]:2022 ([192.168.1.1]:2022)' can't be established.  
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlg0qvGhkHxMkw2sQdblo.  
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.nabakulin.net]:2022' (ED25519) to the list of known hosts.  
nabakulin@server.nabakulin.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Sun Dec  4 03:01:10 2022  
[nabakulin@server.nabakulin.net ~]$
```

Рис. 4

# Результаты выполнения

- Настройте маскардинг на виртуальной машине server для организации доступа клиента к сети Интернет

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

Рис. 6

```
[nabakulin@client.nabakulin.net ~]$ ping ya.ru
PING ya.ru (87.250.250.242) 56(84) bytes of data.
64 bytes from ya.ru (87.250.250.242): icmp_seq=1 ttl=244 time=14.7 ms
64 bytes from ya.ru (87.250.250.242): icmp_seq=2 ttl=244 time=14.0 ms
64 bytes from ya.ru (87.250.250.242): icmp_seq=3 ttl=244 time=13.9 ms
64 bytes from ya.ru (87.250.250.242): icmp_seq=4 ttl=244 time=14.8 ms
64 bytes from ya.ru (87.250.250.242): icmp_seq=5 ttl=244 time=14.3 ms
^C
--- ya.ru ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 10835ms
rtt min/avg/max/mdev = 13.916/14.347/14.806/0.355 ms
```

Рис. 5

# Результаты выполнения

- Напишите скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внести изменения в Vagrantfile

```
#!/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. 7

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

Рис. 8