Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

Факультет информационных технологий и программирования

Практическая работа № 6

Трансляция адресов в ОС Linux

Выполнил студент группы № M3302

Суворин Ярослав Владимирович

Санкт-Петербург
2024

Часть 2. Создание пользователей и настройка OpenSSH Server (sshd).
АРТЕФАКТЫ:
Измененные параметры sshd из Части 2.

```
#LoginGraceTime 30
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 2
#MaxSessions 10
```

```
#UseDNS no
```

Успешно подключились:

```
[root@c9-1 ~]# ssh SYUser@10.0.0.2
SYUser@10.0.0.2's password:
[SYUser@c9-2 ~]$
```

Часть 3. Настройка NAT на шлюзе

АРТЕФАКТЫ:
Итоговые файлы /etc/sysconfig/iptables с хостов c9-1 и c9-2

c9-1:

```
# Generated by iptables-save v1.8.10 (nf_tables) on Sat Nov 30 23:35:47 2024
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [2468:188863]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -j ACCEPT
-A FORWARD -i enp0s3 -o enp0s8 -j ACCEPT
-A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
COMMIT
# Completed on Sat Nov 30 23:35:47 2024
# Generated by iptables-save v1.8.10 (nf_tables) on Sat Nov 30 23:35:47 2024
*nat
:PREROUTING ACCEPT [249:18255]
:INPUT ACCEPT [2:168]
:OUTPUT ACCEPT [305:23031]
:POSTROUTING ACCEPT [4:240]
-A PREROUTING -p tcp -m tcp --dport 55022 -j DNAT --to-destination 10.0.0.2:22
-A POSTROUTING -o enp0s3 -j MASQUERADE
-A POSTROUTING -o enp0s3 -j MASQUERADE
COMMIT
# Completed on Sat Nov 30 23:35:47 2024
```

c9-2

```
# Generated by iptables-save v1.8.10 (nf_tables) on Sat Nov 30 22:28:15 2024
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1299:154110]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Sat Nov 30 22:28:15 2024
# Generated by iptables-save v1.8.10 (nf_tables) on Sat Nov 30 22:28:15 2024
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [11:836]
COMMIT
# Completed on Sat Nov 30 22:28:15 2024
```

Доступ к 8.8.8.8

```
[root@c9-2 ssh]# 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=62 time=50.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=62 time=2.26 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=62 time=2.06 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=62 time=2.15 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=62 time=2.12 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=62 time=2.43 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=62 time=1.87 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=62 time=1.95 ms
```

Часть 4. Установка дополнительного ПО
АРТЕФАКТЫ:
Команда и консольный вывод из Части 4 п.3

```
[root@c9-1 ~]# nmap 10.0.0.2
Starting Nmap 7.92 ( https://nmap.org ) at 2024-12-01 15:07 MSK
Nmap scan report for 10.0.0.2
Host is up (0.00060s latency).
Not shown: 989 filtered tcp ports (no-response), 10 filtered tcp ports (host-prohibited)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:93:F7:1A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.31 seconds
```

Часть 5. Исследование соединений
АРТЕФАКТЫ:
Команды и существенные части консольного вывода Части 5
п. 1
Открытые соединения

```
[root@c9-2 ~]# ss -t -a
State       Recv-Q      Send-Q            Local Address:Port             Peer Address:Port      Process
LISTEN      0           128                     0.0.0.0:ssh                   0.0.0.0:*
LISTEN      0           1024                    0.0.0.0:http                  0.0.0.0:*
```

Открытые сетевые сокеты, ждущие подключения

```
[root@c9-2 ~]# ss -tnl
State          Recv-Q          Send-Q                    Local Address:Port                    Peer Address:Port          Process
LISTEN         0               128                           0.0.0.0:22                           0.0.0.0:*
LISTEN         0               1024                          0.0.0.0:80                           0.0.0.0:*
```

п. 4

Вывод на c9-2

```
                                                  My traceroute  [v0.94]
c9-2 (10.0.0.2) -> ya.ru                                                                    2024-12-01T16:37:39+0300
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                                 Packets               Pings
 Host                                                         Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. _gateway                                                  0.0%     5    5.0   4.1   1.0   5.3   1.8
 2. 10.0.2.2                                                  0.0%     5    1.3   2.8   1.3   7.7   2.7
 3. ya.ru                                                     0.0%     5    2.4   3.9   2.1  10.8   3.8
```

Вывод для enp0s3

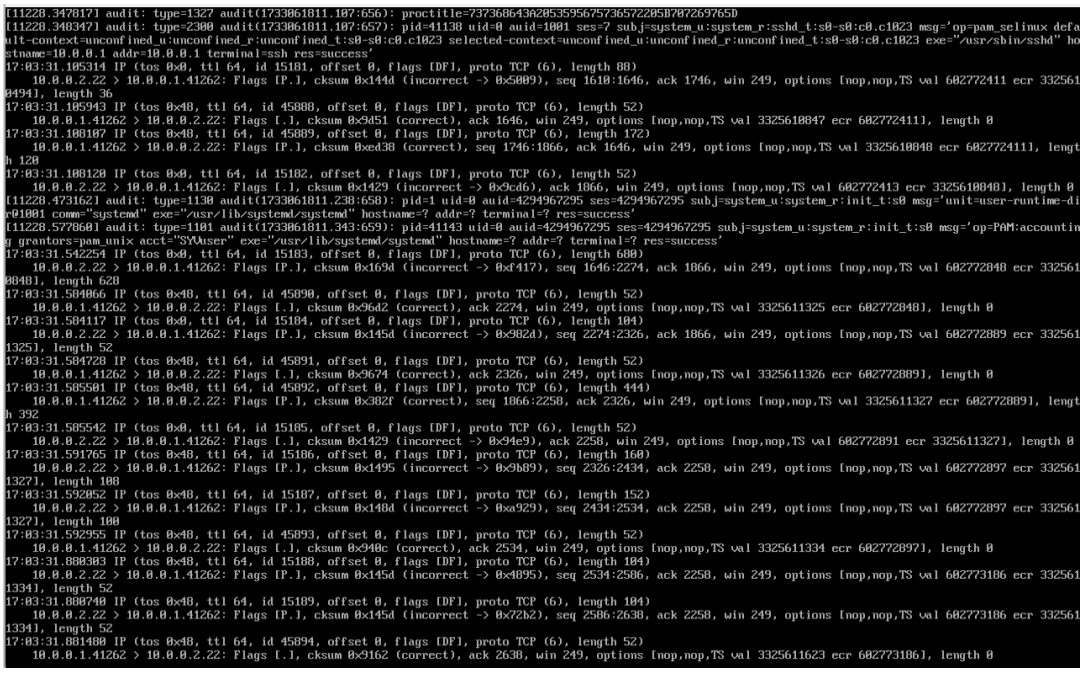
```
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:37:29.090850 IP 10.0.2.15.35186 > 8.8.8.8.53: 31186+ A? ya.ru. (23)
16:37:29.181974 IP 10.0.2.15.35186 > 8.8.8.8.53: 34000+ AAAA? ya.ru. (23)
16:37:29.280670 IP 8.8.8.8.53 > 10.0.2.15.35186: 31186 3/0/0 A 5.255.255.242, A 77.88.44.242, A 77.88.55.242 (71)
16:37:29.280672 IP 8.8.8.8.53 > 10.0.2.15.35186: 34000 1/0/0 AAAA 2a02:6b8::2:242 (51)
16:37:29.496773 IP 10.0.2.15.50539 > 8.8.8.8.53: 41435+ PTR? 1.0.0.10.in-addr.arpa. (39)
16:37:29.583900 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33001, length 64
16:37:29.590809 IP 10.0.2.2 > 10.0.2.15: ICMP time exceeded in-transit, length 36
16:37:29.601178 IP 10.0.2.15.58570 > 8.8.8.8.53: 58591+ PTR? 2.2.0.10.in-addr.arpa. (39)
16:37:29.675384 IP 8.8.8.8.53 > 10.0.2.15.50539: 41435 NXDomain 0/0/0 (39)
16:37:29.684211 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33002, length 64
16:37:29.694248 IP 5.255.255.242 > 10.0.2.15: ICMP echo reply, id 40786, seq 33002, length 64
16:37:29.704681 IP 10.0.2.15.42571 > 8.8.8.8.53: 28042+ PTR? 242.255.255.5.in-addr.arpa. (44)
16:37:29.785172 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33003, length 64
16:37:29.787731 IP 5.255.255.242 > 10.0.2.15: ICMP echo reply, id 40786, seq 33003, length 64
16:37:29.787732 IP 8.8.8.8.53 > 10.0.2.15.58570: 58591 NXDomain 0/0/0 (39)
16:37:29.972925 IP 8.8.8.8.53 > 10.0.2.15.42571: 28042 1/0/0 PTR ya.ru. (63)
16:37:30.454844 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33005, length 64
16:37:30.455169 IP 10.0.2.2 > 10.0.2.15: ICMP time exceeded in-transit, length 36
16:37:30.789714 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33006, length 64
16:37:30.790898 IP 5.255.255.242 > 10.0.2.15: ICMP echo reply, id 40786, seq 33006, length 64
16:37:31.459185 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33008, length 64
16:37:31.459673 IP 10.0.2.2 > 10.0.2.15: ICMP time exceeded in-transit, length 36
16:37:31.793891 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33009, length 64
16:37:31.795027 IP 5.255.255.242 > 10.0.2.15: ICMP echo reply, id 40786, seq 33009, length 64
16:37:32.464630 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33011, length 64
16:37:32.465013 IP 10.0.2.2 > 10.0.2.15: ICMP time exceeded in-transit, length 36
16:37:32.799199 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33012, length 64
16:37:32.800431 IP 5.255.255.242 > 10.0.2.15: ICMP echo reply, id 40786, seq 33012, length 64
16:37:33.468100 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33014, length 64
16:37:33.468405 IP 10.0.2.2 > 10.0.2.15: ICMP time exceeded in-transit, length 36
16:37:33.803503 IP 10.0.2.15 > 5.255.255.242: ICMP echo request, id 40786, seq 33015, length 64
16:37:33.804797 IP 5.255.255.242 > 10.0.2.15: ICMP echo reply, id 40786, seq 33015, length 64
16:37:34.208872 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
16:37:34.209407 ARP, Reply 10.0.2.2 is-at 52:54:00:12:35:02, length 46
16:37:41.104330 IP 10.0.2.15.55123 > 82.65.235.151.123: NTPv4, Client, length 48
16:37:41.298560 IP 82.65.235.151.123 > 10.0.2.15.55123: NTPv4, Server, length 48
16:37:41.888998 IP 10.0.2.15.46185 > 95.31.209.104.123: NTPv4, Client, length 48
16:37:42.184093 IP 95.31.209.104.123 > 10.0.2.15.46185: NTPv4, Server, length 48
16:37:42.473014 IP 10.0.2.15.42247 > 162.159.200.1.123: NTPv4, Client, length 48
16:37:42.653952 IP 162.159.200.1.123 > 10.0.2.15.42247: NTPv4, Server, length 48
16:37:42.758886 IP 10.0.2.15.47099 > 51.195.104.188.123: NTPv4, Client, length 48
16:37:42.956103 IP 51.195.104.188.123 > 10.0.2.15.47099: NTPv4, Server, length 48
```

Вывод для enp0s8

```
istening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
6:37:29.090814 IP 10.0.0.2.35186 > 8.8.8.8.53: 31186+ A? ya.ru. (23)
6:37:29.181949 IP 10.0.0.2.35186 > 8.8.8.8.53: 34000+ AAAA? ya.ru. (23)
6:37:29.280695 IP 8.8.8.8.53 > 10.0.0.2.35186: 31186 3/0/0 A 5.255.255.242, A 77.88.44.242, A 77.88.55.242 (71)
6:37:29.280829 IP 8.8.8.8.53 > 10.0.0.2.35186: 34000 1/0/0 AAAA 2a02:6b8::2:242 (51)
6:37:29.483002 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33000, length 64
6:37:29.483075 IP 10.0.0.1 > 10.0.0.2: ICMP time exceeded in-transit, length 92
6:37:29.496707 IP 10.0.0.2.50539 > 8.8.8.8.53: 41435+ PTR? 1.0.0.10.in-addr.arpa. (39)
6:37:29.583867 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33001, length 64
6:37:29.590822 IP 10.0.2.2 > 10.0.0.2: ICMP time exceeded in-transit, length 36
6:37:29.601164 IP 10.0.0.2.58570 > 8.8.8.8.53: 58591+ PTR? 2.2.0.10.in-addr.arpa. (39)
6:37:29.675406 IP 8.8.8.8.53 > 10.0.0.2.50539: 41435 NXDomain 0/0/0 (39)
6:37:29.684188 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33002, length 64
6:37:29.694267 IP 5.255.255.242 > 10.0.0.2: ICMP echo reply, id 40786, seq 33002, length 64
6:37:29.704659 IP 10.0.0.2.42571 > 8.8.8.8.53: 28042+ PTR? 242.255.255.5.in-addr.arpa. (44)
6:37:29.785147 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33003, length 64
6:37:29.787743 IP 5.255.255.242 > 10.0.0.2: ICMP echo reply, id 40786, seq 33003, length 64
6:37:29.787857 IP 8.8.8.8.53 > 10.0.0.2.58570: 58591 NXDomain 0/0/0 (39)
6:37:29.972976 IP 8.8.8.8.53 > 10.0.0.2.42571: 28042 1/0/0 PTR ya.ru. (63)
6:37:30.119621 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33004, length 64
6:37:30.119656 IP 10.0.0.1 > 10.0.0.2: ICMP time exceeded in-transit, length 92
6:37:30.454674 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33005, length 64
6:37:30.455184 IP 10.0.2.2 > 10.0.0.2: ICMP time exceeded in-transit, length 36
6:37:30.789657 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33006, length 64
6:37:30.790909 IP 5.255.255.242 > 10.0.0.2: ICMP echo reply, id 40786, seq 33006, length 64
6:37:31.124552 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33007, length 64
6:37:31.124635 IP 10.0.0.1 > 10.0.0.2: ICMP time exceeded in-transit, length 92
6:37:31.459104 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33008, length 64
6:37:31.459685 IP 10.0.2.2 > 10.0.0.2: ICMP time exceeded in-transit, length 36
6:37:31.793833 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33009, length 64
6:37:31.795039 IP 5.255.255.242 > 10.0.0.2: ICMP echo reply, id 40786, seq 33009, length 64
6:37:32.128952 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33010, length 64
6:37:32.129026 IP 10.0.0.1 > 10.0.0.2: ICMP time exceeded in-transit, length 92
6:37:32.464558 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33011, length 64
6:37:32.465023 IP 10.0.2.2 > 10.0.0.2: ICMP time exceeded in-transit, length 36
6:37:32.799142 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33012, length 64
6:37:32.800443 IP 5.255.255.242 > 10.0.0.2: ICMP echo reply, id 40786, seq 33012, length 64
6:37:33.133886 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33013, length 64
6:37:33.133931 IP 10.0.0.1 > 10.0.0.2: ICMP time exceeded in-transit, length 92
6:37:33.468067 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33014, length 64
6:37:33.468417 IP 10.0.2.2 > 10.0.0.2: ICMP time exceeded in-transit, length 36
6:37:33.803449 IP 10.0.0.2 > 5.255.255.242: ICMP echo request, id 40786, seq 33015, length 64
6:37:33.804807 IP 5.255.255.242 > 10.0.0.2: ICMP echo reply, id 40786, seq 33015, length 64
6:37:34.322333 ARP, Request who-has 10.0.0.1 tell 10.0.0.2, length 46
6:37:34.322377 ARP, Reply 10.0.0.1 is-at 08:00:27:f7:08:a2, length 28
```

п. 6,8

```
tart direction=from-server cipher=aes256-gcm@openssh.com ksize=256 mac=<implicit> pfs=curve25519-sha256 spid=41139 suid=74 rport=41262 laddr=10.0.0.2 lport=22
exe="/usr/sbin/sshd" hostname=? addr=10.0.0.1 terminal=? res=success'
[11205.568433] audit: type=2407 audit(1733861788.336:651): pid=41138 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=s
tart direction=from-client cipher=aes256-gcm@openssh.com ksize=256 mac=<implicit> pfs=curve25519-sha256 spid=41139 suid=74 rport=41262 laddr=10.0.0.2 lport=22
exe="/usr/sbin/sshd" hostname=? addr=10.0.0.1 terminal=? res=success'
17:03:08.236000 IP (tos 0x0, ttl 64, id 15170, offset 0, flags [DF], proto TCP (6), length 73)
    10.0.0.2.22 > 10.0.0.1.41262: Flags [P.], cksum 0x143e (incorrect -> 0x956b), seq 1:22, ack 22, win 249, options [nop,nop,TS val 602749541 ecr 3325587967],
length 21: SSH: SSH-2.0-OpenSSH_8.7
17:03:08.236522 IP (tos 0x48, ttl 64, id 45880, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.1.41262 > 10.0.0.2.22: Flags [.], cksum 0x5d0f (correct), ack 22, win 251, options [nop,nop,TS val 3325587978 ecr 602749541], length 0
17:03:08.237426 IP (tos 0x48, ttl 64, id 45881, offset 0, flags [DF], proto TCP (6), length 1444)
    10.0.0.1.41262 > 10.0.0.2.22: Flags [P.], cksum 0x26c2 (correct), seq 22:1414, ack 22, win 251, options [nop,nop,TS val 3325587979 ecr 602749541], length 13
92
17:03:08.284762 IP (tos 0x0, ttl 64, id 15171, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.2.22 > 10.0.0.1.41262: Flags [.], cksum 0x1429 (incorrect -> 0x576f), ack 1414, win 249, options [nop,nop,TS val 602749590 ecr 3325587979], length 0
17:03:08.336157 IP (tos 0x0, ttl 64, id 15172, offset 0, flags [DF], proto TCP (6), length 1020)
    10.0.0.2.22 > 10.0.0.1.41262: Flags [P.], cksum 0x17f1 (incorrect -> 0x302e), seq 22:990, ack 1414, win 249, options [nop,nop,TS val 602749642 ecr 332558797
9], length 968
17:03:08.338078 IP (tos 0x48, ttl 64, id 45882, offset 0, flags [DF], proto TCP (6), length 100)
    10.0.0.1.41262 > 10.0.0.2.22: Flags [P.], cksum 0xa051 (correct), seq 1414:1462, ack 990, win 249, options [nop,nop,TS val 3325588080 ecr 602749642], length
 48
17:03:08.338901 IP (tos 0x0, ttl 64, id 15173, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.2.22 > 10.0.0.1.41262: Flags [.], cksum 0x1429 (incorrect -> 0x52dc), ack 1462, win 249, options [nop,nop,TS val 602749644 ecr 3325588080], length 0
17:03:08.342329 IP (tos 0x0, ttl 64, id 15174, offset 0, flags [DF], proto TCP (6), length 536)
    10.0.0.2.22 > 10.0.0.1.41262: Flags [P.], cksum 0x160d (incorrect -> 0xd5b2), seq 990:1474, ack 1462, win 249, options [nop,nop,TS val 602749648 ecr 3325588
080], length 484
17:03:08.346061 IP (tos 0x48, ttl 64, id 45883, offset 0, flags [DF], proto TCP (6), length 68)
    10.0.0.1.41262 > 10.0.0.2.22: Flags [P.], cksum 0x46b4 (correct), seq 1462:1478, ack 1474, win 249, options [nop,nop,TS val 3325588087 ecr 602749648], lengt
h 16
17:03:08.387425 IP (tos 0x0, ttl 64, id 15175, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.2.22 > 10.0.0.1.41262: Flags [.], cksum 0x1429 (incorrect -> 0x50b0), ack 1478, win 249, options [nop,nop,TS val 602749693 ecr 3325588087], length 0
17:03:08.397766 IP (tos 0x48, ttl 64, id 45884, offset 0, flags [DF], proto TCP (6), length 104)
    10.0.0.1.41262 > 10.0.0.2.22: Flags [P.], cksum 0xb3f8 (correct), seq 1478:1530, ack 1474, win 249, options [nop,nop,TS val 3325588129 ecr 602749693], lengt
h 52
17:03:08.397790 IP (tos 0x0, ttl 64, id 15176, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.2.22 > 10.0.0.1.41262: Flags [.], cksum 0x1429 (incorrect -> 0x5048), ack 1530, win 249, options [nop,nop,TS val 602749703 ecr 3325588129], length 0
17:03:08.441036 IP (tos 0x0, ttl 64, id 15177, offset 0, flags [DF], proto TCP (6), length 104)
    10.0.0.2.22 > 10.0.0.1.41262: Flags [P.], cksum 0x145d (incorrect -> 0xca10), seq 1474:1526, ack 1530, win 249, options [nop,nop,TS val 602749746 ecr 332558
8129], length 52
17:03:08.441763 IP (tos 0x48, ttl 64, id 45885, offset 0, flags [DF], proto TCP (6), length 120)
    10.0.0.1.41262 > 10.0.0.2.22: Flags [P.], cksum 0xa357 (correct), seq 1530:1598, ack 1526, win 249, options [nop,nop,TS val 3325588183 ecr 602749746], lengt
h 68
17:03:08.441783 IP (tos 0x0, ttl 64, id 15178, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.2.22 > 10.0.0.1.41262: Flags [.], cksum 0x1429 (incorrect -> 0x4f6e), ack 1598, win 249, options [nop,nop,TS val 602749747 ecr 3325588183], length 0
17:03:08.451750 IP (tos 0x0, ttl 64, id 15179, offset 0, flags [DF], proto TCP (6), length 136)
    10.0.0.2.22 > 10.0.0.1.41262: Flags [P.], cksum 0x147d (incorrect -> 0xd4d4), seq 1526:1610, ack 1598, win 249, options [nop,nop,TS val 602749757 ecr 332558
8183], length 84
17:03:08.500733 IP (tos 0x48, ttl 64, id 45886, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.1.41262 > 10.0.0.2.22: Flags [.], cksum 0x4edc (correct), ack 1610, win 249, options [nop,nop,TS val 3325588235 ecr 602749757], length 0
s
```



Часть 6. Настройка шлюза
АРТЕФАКТЫ:
Текст итоговых правил iptables с c7-1

```
# Generated by iptables-save v1.8.10 (nf_tables) on Sun Dec  1 18:59:52 2024
*mangle
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed on Sun Dec  1 18:59:52 2024
# Generated by iptables-save v1.8.10 (nf_tables) on Sun Dec  1 18:59:52 2024
*raw
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT
# Completed on Sun Dec  1 18:59:52 2024
# Generated by iptables-save v1.8.10 (nf_tables) on Sun Dec  1 18:59:52 2024
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [428:38828]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 192.168.1.0/24 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 192.56.0.11/32 -j DROP
-A INPUT -s 14.12.0.0/18 -j DROP
-A INPUT -i enp0s3 -p tcp -m tcp --dport 22 -j DROP
-A INPUT -s 10.0.0.0/24 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j DROP
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A FORWARD -j ACCEPT
-A FORWARD -i enp0s3 -o enp0s8 -j ACCEPT
-A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
-A FORWARD -s 10.0.0.0/24 -d 8.8.8.8/32 -p udp -m udp --dport 53 -j ACCEPT
-A FORWARD -s 10.0.0.0/24 -d 77.88.8.1/32 -p udp -m udp --dport 53 -j ACCEPT
-A FORWARD -s 10.0.0.0/24 -p tcp -m tcp --dport 110 -j ACCEPT
-A FORWARD -s 10.0.0.0/24 -p tcp -m multiport --dports 80,443,8080 -j ACCEPT
-A FORWARD -s 10.0.0.0/24 -p tcp -m tcp --dport 22 -j ACCEPT
-A FORWARD -s 10.0.0.0/24 -d 192.168.1.0/24 -p tcp -m tcp --dport 25 -j ACCEPT
-A FORWARD -s 14.12.0.0/18 -j DROP
-A FORWARD -s 192.56.0.11/32 -j DROP
-A FORWARD -s 10.0.0.0/24 -d 8.8.8.8/32 -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
```

```
COMMIT
# Completed on Sun Dec  1 18:59:52 2024
# Generated by iptables-save v1.8.10 (nf_tables) on Sun Dec  1 18:59:52 2024
*nat
:PREROUTING ACCEPT [265:19701]
:INPUT ACCEPT [2:197]
:OUTPUT ACCEPT [247:18478]
:POSTROUTING ACCEPT [5:300]
-A PREROUTING -p tcp -m tcp --dport 55022 -j DNAT --to-destination 10.0.0.2:22
-A POSTROUTING -o enp0s3 -j MASQUERADE
-A POSTROUTING -o enp0s3 -j MASQUERADE
COMMIT
# Completed on Sun Dec  1 18:59:52 2024
```

Часть 7. Доступ через ssh к защищенным сервисам

АРТЕФАКТЫ:

Команда подключения из Части 7, п.1.

```
C:\Users\y2008>ssh -L 127.0.0.80:8888:127.0.0.1:80 SYVuser@localhost -p 55022
```

1. В чем разница между действиями SNAT или MASQUERADE? Когда уместно использовать одно, а когда другое?

SNAT (Source Network Address Translation): Это трансляция исходных IP-адресов для исходящих пакетов. SNAT обычно используется в ситуациях, когда маршрутизатор или шлюз имеет статический IP-адрес и требуется изменить исходный IP-адрес исходящих пакетов на IP этого маршрутизатора.

MASQUERADE: Маскарадинг является разновидностью SNAT, но с тем отличием, что используется динамический IP-адрес. Это автоматически подстраивает исходящий адрес, если внешний интерфейс получает новый IP.

Использование:

- SNAT: Если статический IP-адрес
- MASQUERADE: Если динамический IP-адрес

2. Какие цепочки и какие таблицы существуют в iptables по умолчанию?

Таблицы:

1. filter (по умолчанию): Эта таблица используется для фильтрации пакетов (разрешать или блокировать).
    - Цепочки: INPUT, OUTPUT, FORWARD
2. nat: Используется для трансляции адресов (например, SNAT, DNAT).
    - Цепочки: PREROUTING, POSTROUTING, OUTPUT
3. mangle: Используется для изменения пакетов (например, для изменения TTL, маркеров).
    - Цепочки: PREROUTING, POSTROUTING, INPUT, OUTPUT, FORWARD
4. raw: Таблица для принятия решений о том, стоит ли отслеживать соединение или нет (используется для отключения отслеживания соединений).
    - Цепочки: PREROUTING, OUTPUT
5. security: Таблица для настроек безопасности SELinux.
    - Цепочки: INPUT, OUTPUT, FORWARD

Цепочки по умолчанию в таблице filter:

- INPUT: Обрабатывает пакеты, предназначенные для локальной машины.
- OUTPUT: Обрабатывает пакеты, отправляемые из локальной машины.
- FORWARD: Обрабатывает пакеты, которые проходят через машину (то есть не предназначены для нее).

3. Как добавить новую цепочку? Как перенаправить в нее трафик?
Новая цепочка:
iptables -N <цепочка>
Перенаправление трафика:
sudo iptables -A <исх. цепочка> -j <цепочка>
4. Имеет ли смысл порядок правил?
Да, порядок правил имеет значение, потому что iptables обрабатывает пакеты поочередно, начиная с верхнего правила. Если пакет совпадает с правилом, дальнейшая проверка не происходит. Например, если первое правило разрешает все пакеты, то последующие правила не будут проверяться, и пакет будет пропущен.
5. Как с помощью iptables можно реализовать настройки, при которых брандмауэр пропускает пакеты тех соединений, которые были инициированы изнутри. Учтите, что

правило позволяло установить соединение, т.е. передать пакеты наружу, так и получать ответы, то есть принять ответные пакеты.
Разрешение исходящих соединений
iptables -A OUTPUT -j ACCEPT
Разрешение ответных пакетов на исходящие соединения
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
Блокировка остальных пакетов
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT