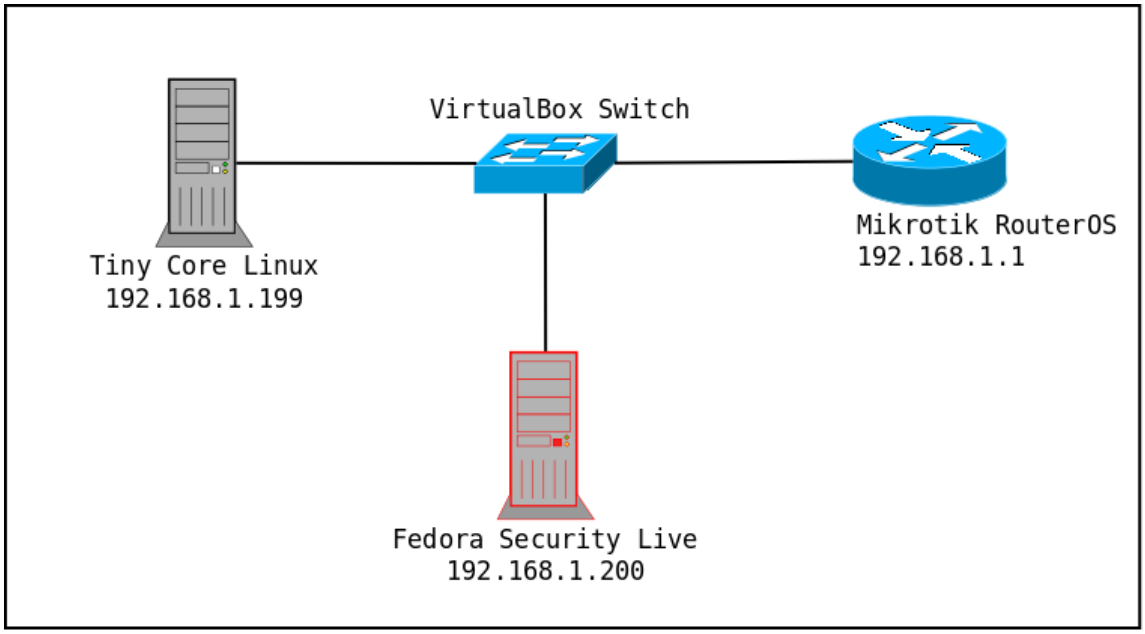
Практические задания
(безопасность сетевого и транспортного уровня)

Для выполнения заданий будет использоваться следующая конфигурация:



Компьютер злоумышленника – дистрибутив для тестирования безопасности Fedora Security Live (FSL).
Маршрутиатор – Mikrotik RouterOS
Пользователь локальной сети – Tiny Core Linux
На всех VM сетевые интерфейсы находятся в режиме Internal Net

Адреса могут быть назначены статически или динамически по протоколу DHCP.
Пример натроек DHCP-сервера в Mikrotik:

```
[admin@MikroTik] > ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: ether1
Select network for DHCP addresses

dhcp address space: 192.168.1.0/24
Select gateway for given network

gateway for dhcp network: 192.168.1.1
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.1.100-192.168.1.200
Select DNS servers

dns servers: 192.168.1.1
Select lease time

lease time: 10m
[admin@MikroTik] >
```

Настройки для TinyCore Linux

```
tc@box:~$ sudo ifconfig eth0 192.168.1.199 netmask 255.255.255.0 up
tc@box:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:D5:47:FA
          inet addr:192.168.1.199  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4982 (4.8 KiB)  TX bytes:6156 (6.0 KiB)
          Interrupt:10 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Настройки для Mikrotik RouterOS:

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.1.1/24     192.168.1.0     ether1
```

Настройки для Fedora Security Live:

```
[liveuser@localhost-live ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.200  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::7e2f:b574:bb10:cee5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a3:c8:22  txqueuelen 1000  (Ethernet)
        RX packets 27  bytes 7242 (7.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 122  bytes 21508 (21.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 63  bytes 6921 (6.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 63  bytes 6921 (6.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Задание 1. Сканирование сети

С помощью программы nmap с рабочего места злоумышленника выявите узлы в локальной сети, определите работающие сервисы, их версии.

Выявление “живых” хостов в сети с помощью ICMP-сканирования:

```
# nmap -sP 192.168.1.0/24
```

```
[liveuser@localhost-live ~]$ nmap -sP 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-03 05:15 EDT
Nmap scan report for _gateway (192.168.1.1)
Host is up (0.016s latency).
Nmap scan report for 192.168.1.199
Host is up (0.0019s latency).
Nmap scan report for localhost-live (192.168.1.200)
Host is up (0.00035s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 12.74 seconds
```

В результате сканирования выявлено 3 узла: 192.168.1.1, 192.168.1.199, 192.168.1.200

```
# nmap -A 192.168.1.1 -oN result.txt -v
```

Результаты сканирования сетевых сервисов для узла 192.168.1.1:

```
Nmap scan report for _gateway (192.168.1.1)
Host is up (0.0014s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            MikroTik router ftpd 6.47.9
| ftp-syst:
|   SYST: UNIX MikroTik 6.47.9
|   STAT:
|  MikroTik FTP server (MikroTik 6.47.9) status:
| Logged in as
| TYPE: ASCII; STRUcture: File; transfer MODE: Stream
| No data connection
|_End of status
22/tcp   open  ssh            MikroTik RouterOS sshd (protocol 2.0)
| ssh-hostkey:
|   1024 1b:78:a3:7c:dd:5b:a4:a1:af:e2:c4:87:96:9c:f9:a9 (DSA)
|_  2048 fc:b4:3d:19:ea:fc:56:a3:66:e3:0c:86:f0:f6:89:06 (RSA)
23/tcp   open  telnet         Linux telnetd
80/tcp   open  http           MikroTik router config httpd
|_http-favicon: Unknown favicon MD5: 77B2F4C09890AB658A72C4BAD8C1077B
| http-methods:
|_  Supported Methods: GET HEAD
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: RouterOS router configuration page
2000/tcp open  bandwidth-test MikroTik bandwidth-test server
8291/tcp open  unknown
Service Info: OSs: Linux, RouterOS; Device: router; CPE: cpe:/o:mikrotik:routeros,
```

Осуществить SYN-сканирование с помощью утилиты hping3:

```
# hping3 --scan 1-65535 -S 192.168.1.1
```

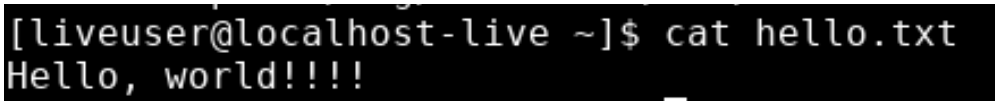
```
Scanning 192.168.1.1 (192.168.1.1), port 1-65535
65535 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   21 ftp        : .S..A...  64     0 14600    46
   22 ssh        : .S..A...  64     0 14600    46
   23 telnet     : .S..A...  64     0 14600    46
   80 http       : .S..A...  64     0 14600    46
 2000 sieve-filte: .S..A...  64     0 14600    46
 8291            : .S..A...  64     0 14600    46
 8728            : .S..A...  64     0 14600    46
 8729            : .S..A...  64     0 14600    46
All replies received. Done.
Not responding ports:
```

С помощью утилиты netcat откроем UDP-порт на узле 192.168.1.199 и проверим с помощью hping3 его работоспособность:

```
# nc -l -u -p 2000
```

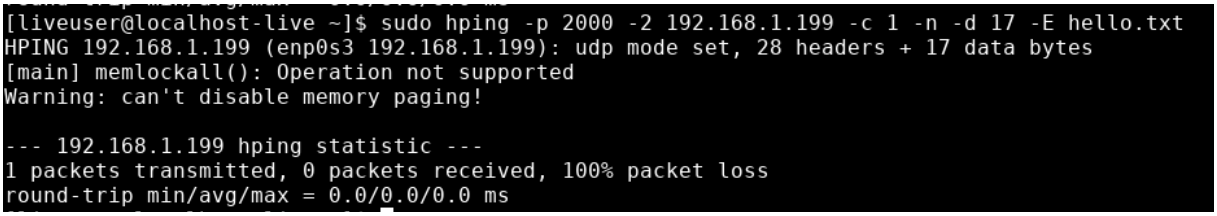
Для этого создадим произвольный файл, например, hello.txt

Содержимое файла:

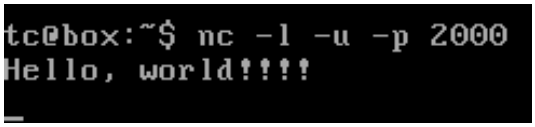


Отправим содержимое файла в UDP-дейтаграмме на порт 2000:

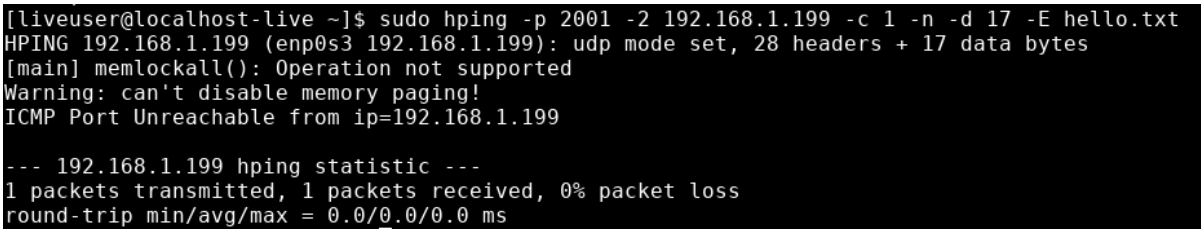
```
# hping3 -p 2000 -2 192.168.1.199 -c 1 -n -d 17 -E hello.txt
```



Проверим получение данных:



При отправке аналогичных данных на закрытый порт 2001 будет получено ICMP сообщение Port Unreachable:

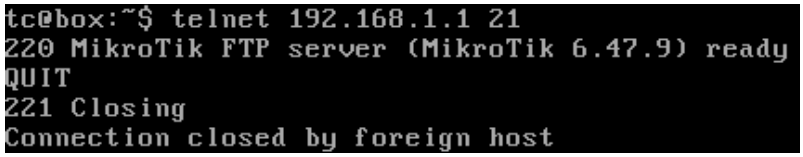


Задание 2. Осуществление DoS-атаки на сетевой сервис

С помощью утилиты hping3 осуществить SYN-flood атаку на FTP-сервис маршрутизатора Mikrotik

Исходное состояние – проверить доступность FTP-сервера с TinyCore Linux с помощью telnet:

```
$ telnet 192.168.1.1 21
```



Запустить DoS-атаку типа SYN-flood:

```
$ hping3 --flood -p 21 -S 192.168.1.1
```

```
[liveuser@localhost-live ~]$ sudo hping3 --flood -p 21 -S 192.168.1.1
HPING 192.168.1.1 (enp0s3 192.168.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Через 30 секунд убедиться, что клиенту с tiny core Linux не удается подключиться к серверу FTP:

```
tc@box:~$ telnet 192.168.1.1 21
telnet: can't connect to remote host (192.168.1.1): Connection timed out
```

Отключить атаку и убедиться, что сервис снова стал доступен.

Задание 3. Выявление и блокирование SYN-flood атаки на устройстве Mikrotik

В Mikrotik добавить правила:

```
/ip firewall filter

add action=jump chain=input connection-state=new protocol=tcp tcp-flags=syn jump-target=detect-ddos

add action=drop chain=input connection-state=new src-address-list=ddoser

add action=return chain=detect-ddos dst-limit=15,15,src-address/10s

add action=add-src-to-address-list chain=detect-ddos address-list=ddoser address-list-timeout=1m
```

```
[admin@MikroTik] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=input action=jump jump-target=detect-ddos tcp-flags=syn
      connection-state=new protocol=tcp

 1    chain=input action=drop connection-state=new src-address-list=ddoser

 2    chain=detect-ddos action=return dst-limit=15,15,src-address/10s

 3    chain=detect-ddos action=add-src-to-address-list address-list=ddoser
      address-list-timeout=1m
```

Повторить атаку из задания 2.

Проверить возможность подключения клиентов к FTP-серверу во время атаки:

```
$ telnet 192.168.1.1 21
```

```
tc@box:~$ telnet 192.168.1.1 21
220 MikroTik FTP server (MikroTik 6.47.9) ready
QUIT
221 Closing
Connection closed by foreign host
```

Проверить наличие IP-адреса злоумышленника в списке ddoser.

```
[admin@MikroTik] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #    LIST                ADDRESS                                 CREATION-TIME
 0 D  ddoser              192.168.1.200                           may/05/2021 08:23:06
```