

Міністерство освіти і науки України
Львівський національний університет імені Івана Франка

Факультет електроніки та комп'ютерних технологій

Кафедра оптоелектроніки
та інформаційних технологій

Звіт

Про виконання лабораторної роботи №3
3 курсу «Комп'ютерні інформаційні мережі»
«Безпека мережі»

Виконав:
Студент групи ФеС-21
Шавало Андрій
Викладач: асист. Галяткін О. О.

Львів-2025

Тема: Безпека мережі.

Мета роботи: аналіз методів боротьби з різними видами мережевих атак та практична реалізація елементів політики мережевої безпеки (налаштування firewall, встановлення та налаштування VPN сервера).

Хід роботи

1. Налаштувати firewall (iptables) на віртуальному сервері з урахуванням завдань попередньої лабораторної роботи за такими параметрами:

a. Обмежити можливість підключення по протоколу SSH тільки з вашої IP адреси.

b. Дозволити доступ до веб сервера (http і https).

```
andriy@sos:~$ curl ifconfig.me
188.163.113.195andriy@sos:~$ sudo iptables -A INPUT -p tcp --dport 22 -s 188.163.113.195 -j ACCEPT
andriy@sos:~$ sudo iptables -A INPUT -p tcp --dport 22 -j REJECT
andriy@sos:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
andriy@sos:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

2. Встановити та налаштувати VPN сервер (OpenVPN)

```
andriy@sos:~$ wget https://git.io/vpn -O openvpn-install.sh
```

```
andriy@sos:~$ chmod +x openvpn-install.sh
andriy@sos:~$ sudo ./openvpn-install.sh
```

```
This server is behind NAT. What is the public IPv4 address or hostname?
Public IPv4 address / hostname [188.163.113.195]:

Which protocol should OpenVPN use?
  1) UDP (recommended)
  2) TCP
Protocol [1]: 1

What port should OpenVPN listen to?
Port [1194]:

Select a DNS server for the clients:
  1) Current system resolvers
  2) Google
  3) 1.1.1.1
  4) OpenDNS
  5) Quad9
  6) AdGuard
DNS server [1]:

Enter a name for the first client:
Name [client]: andriy
```

3. Продемонструвати роботу VPN сервера за допомогою утиліт traceroute чи mtr

```
andriy@sos:~$ sudo openvpn --config /root/andriy.ovpn

andriy@sos:~$ traceroute 172.17.0.0
traceroute to 172.17.0.0 (172.17.0.0), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  21.514 ms  0.624 ms  0.645 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  *
 * *
```

4. Налаштувати VPN таким чином, щоб тільки трафік в мережу 172.17.0.0/24 попадав у VPN тунель.

```
andriy@sos:~$ ip route
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
10.8.0.0/24 dev tun0 proto kernel scope link src 10.8.0.1
172.17.0.0/24 via 10.8.0.1 dev tun0
```

Висновок:

У результаті виконання налаштування OpenVPN, трафік до мережі 172.17.0.0/24 тепер проходить через VPN тунель, забезпечуючи безпечний доступ до цієї мережі. Інший трафік не перенаправляється через тунель і використовує звичайне інтернет-з'єднання. Це дозволяє ефективно обмежити доступ лише до конкретної мережі через VPN, що підвищує безпеку та зменшує навантаження на тунель для інших типів трафіку.