Кам’янець-Подільський національний університет імені Івана Огієнка

Кафедра комп’ютерних наук

Навчальна дисципліна

**«Технології захисту інформації»**

Лабораторна робота №6

Конфігурація мережевої безпеки (iptables, OpenVPN, sslscan)

Виконав:

студент 4-го курсу

групи KN1-B22

**Демченко Дмитро**

Кам’янець-Подільський – 2025

**Мета:** налаштувати базовий firewall, встановити OpenVPN-клієнт, перевірити SSL.

**Опис середовища:**

ПЗ для віртуальної машини: VMware® Workstation 17 Pro 17.6.4 build-24832109, iptables v1.8.11 (nf\_tables), OpenVPN 2.6.14 x86\_64-pc-linux-gnu, sslscan 2.1.5,OpenSSL 3.5.2 5 Aug 2025, Local Kali ip: 192.168.135.130

**Команди:**

1) Правила iptables:

sudo iptables -F

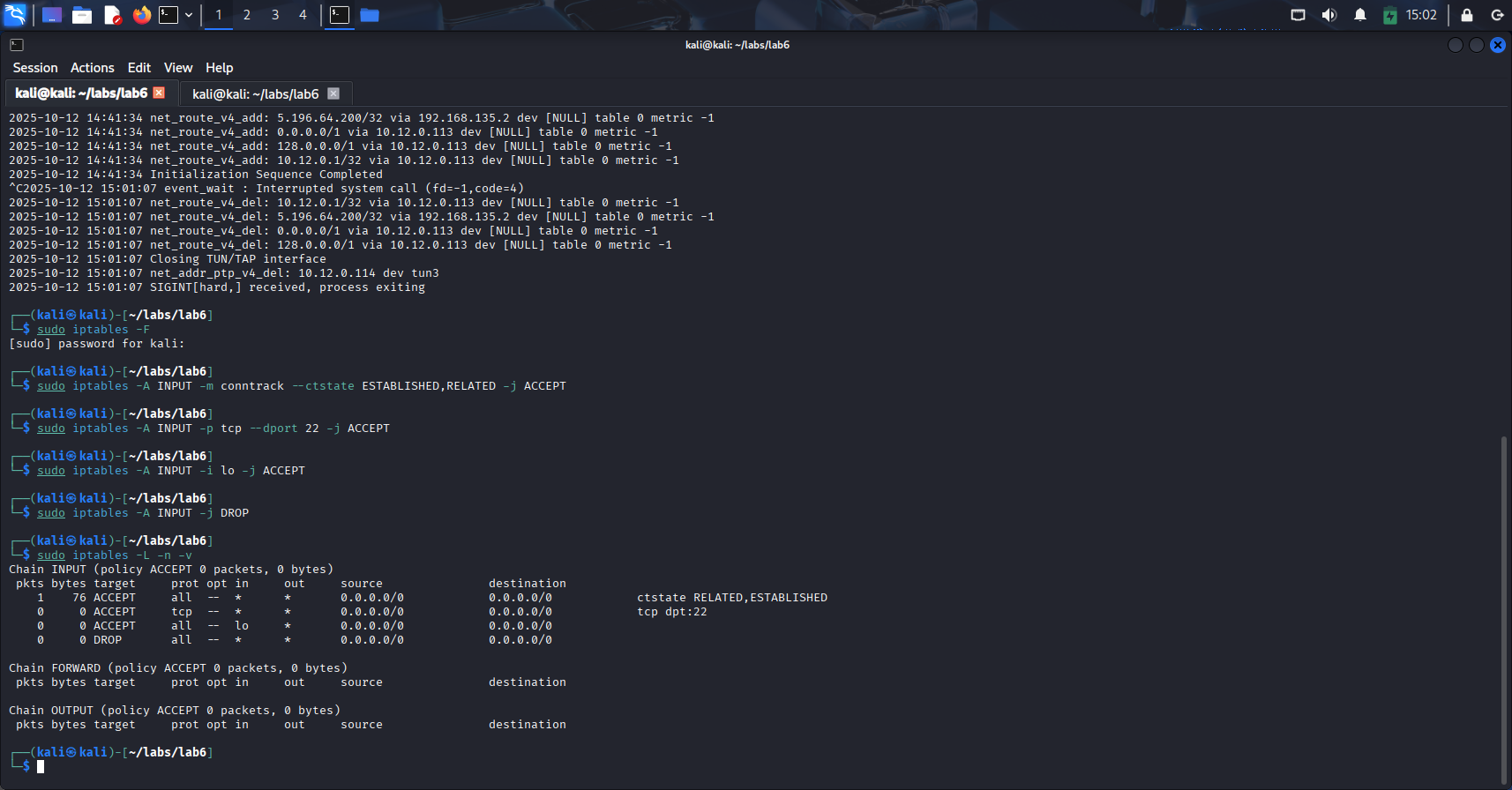
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

sudo iptables -A INPUT -i lo -j ACCEPT

sudo iptables -A INPUT -j DROP

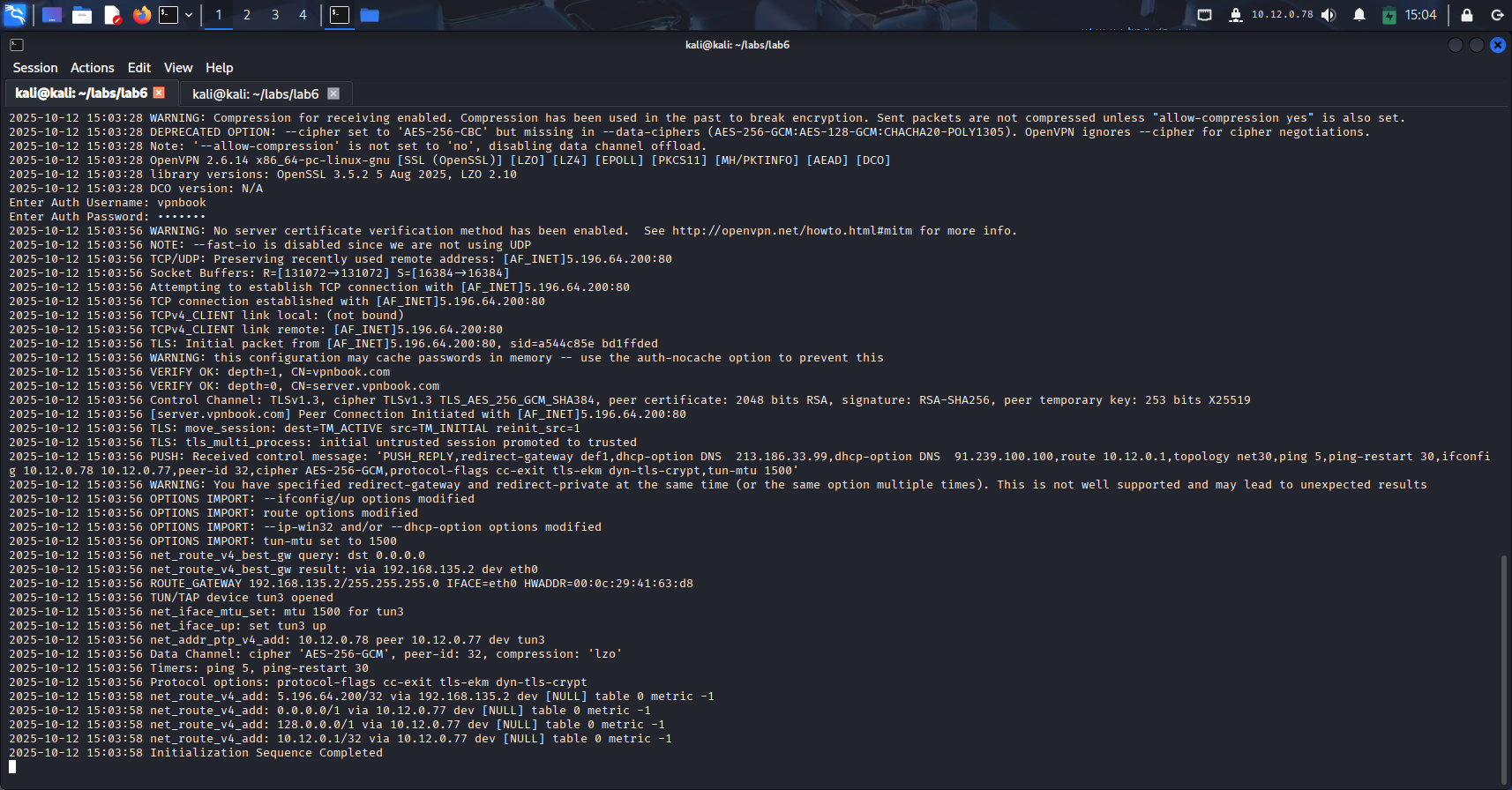
sudo iptables -L -n -v

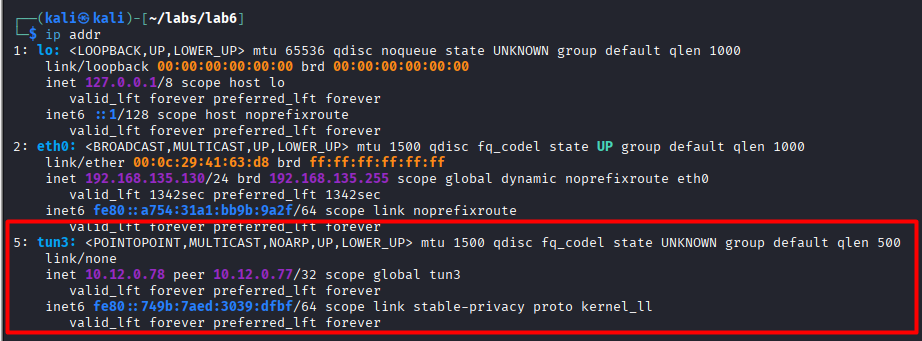


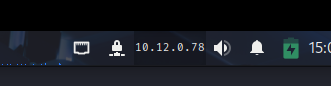
2) Підключення OpenVPN:

sudo openvpn --config client.ovpn

Використав готовий файл конфігурації з сайту VPNBook.



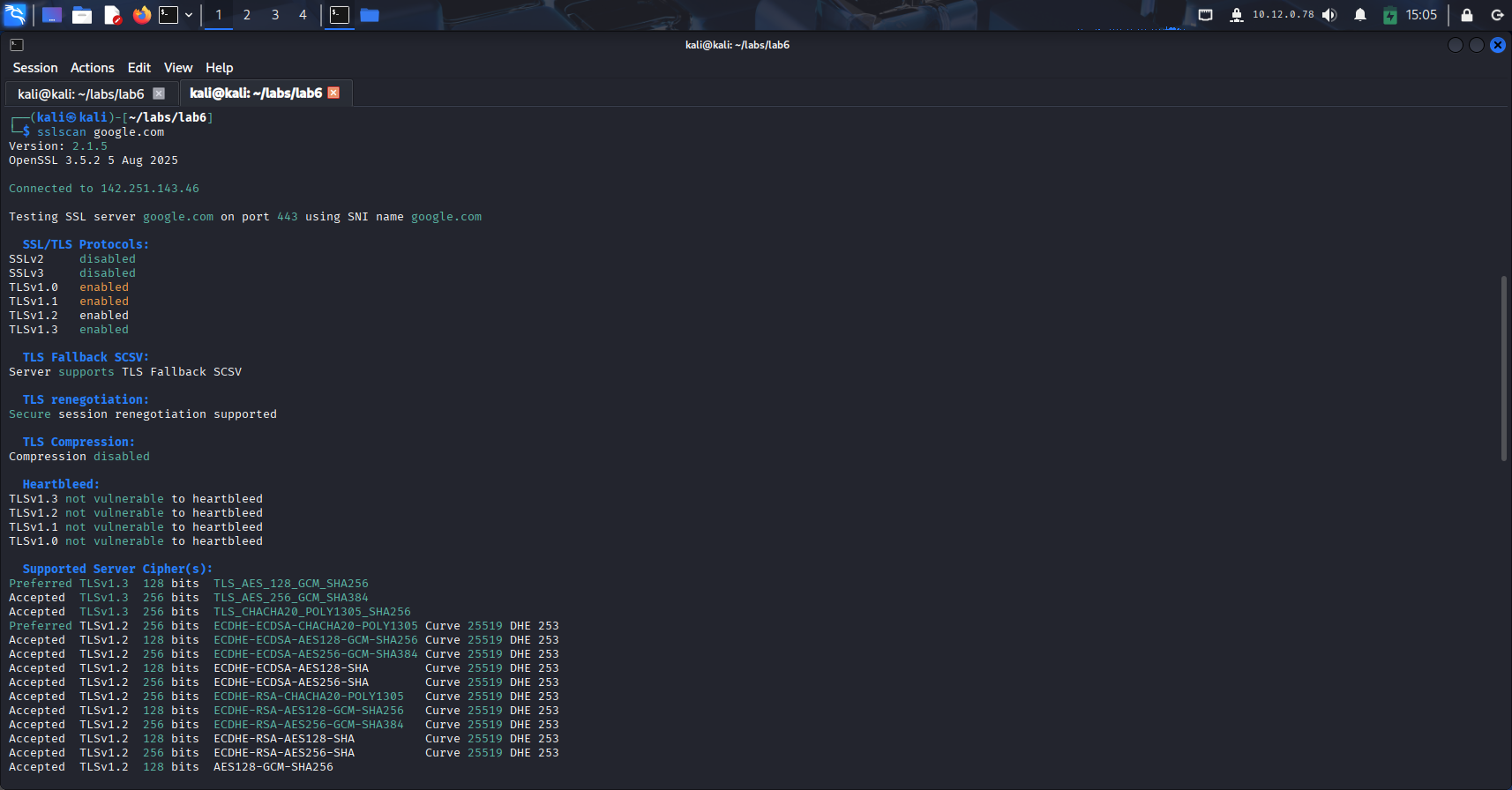


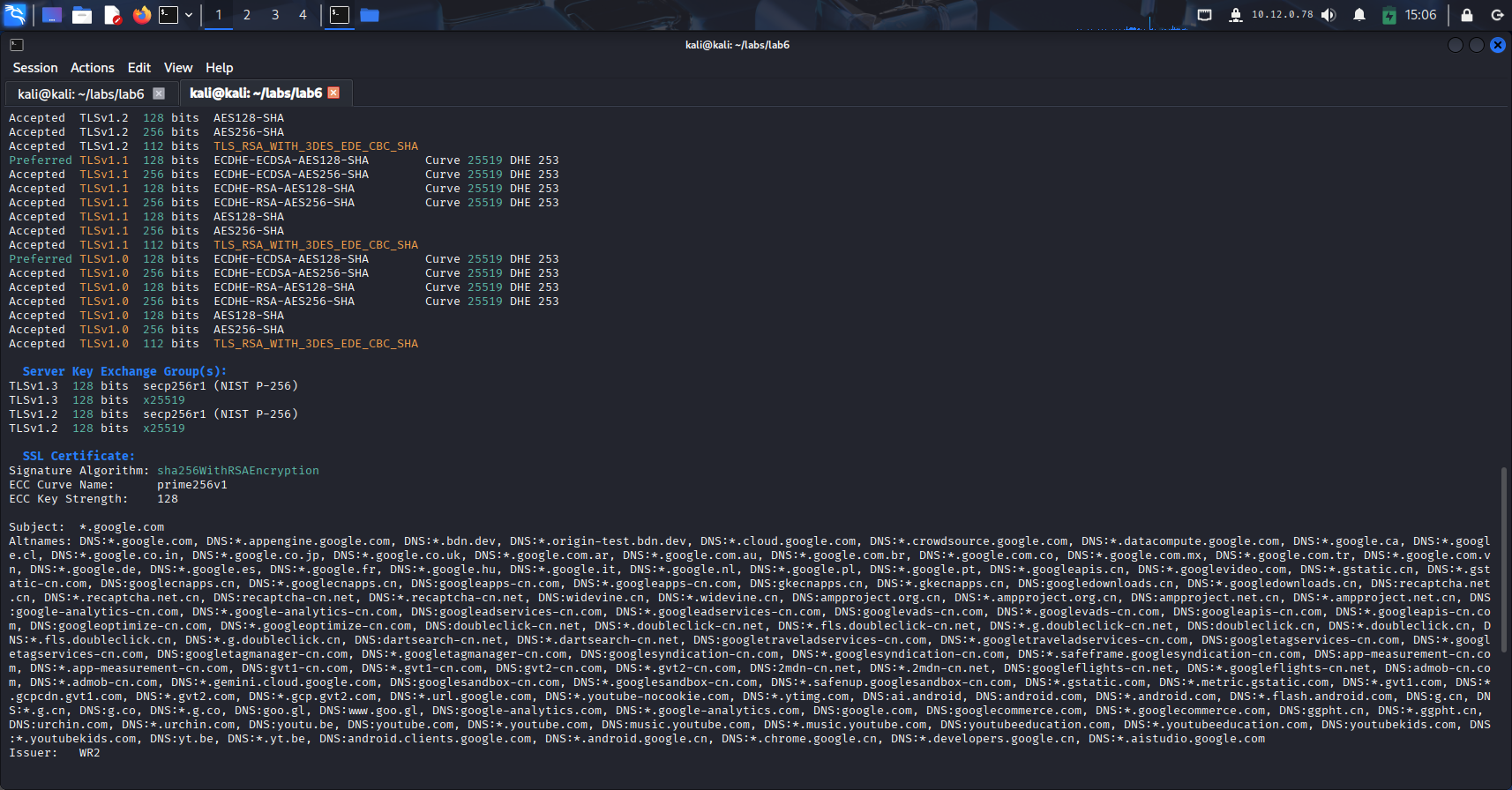


3) SSL перевірка:

sslscan <hostname>

Спроба просканувати SSL на локальному хості, який розташований на іншій віртуальній машині за допомогою sslscan завершилася помилкою Connection refused. Це вказало на те, що на цільовій машині на стандартному порту 443 не було запущено жодного сервісу, який міг би прийняти з'єднання. Тому просканував google.com.





**Висновки:** Під час виконання лабораторної роботи №6 я успішно налаштував базові правила фаєрволу за допомогою iptables, що дозволило контролювати вхідний трафік на віртуальній машині, ініціалізував та налаштував OpenVPN, перевірив SSL.