Лабораторна робота №9

Тема: Забезпечення безпеки мережі з WireGuard

Мета:

- Ознайомитися з сучасним підходом до створення захищених з'єднань у комп’ютерних мережах.
- Вивчити принципи роботи VPN-протоколу WireGuard.
- Налаштувати захищене VPN-з’єднання між сервером та клієнтом за допомогою WireGuard.

Хід роботи

1. **Теоретична підготовка**
   - Вивчити архітектуру та принципи роботи WireGuard: криптографія, тунелювання, обмін ключами.
   - Порівняти WireGuard з іншими VPN-рішеннями (OpenVPN, IPSec тощо).
2. **Інсталяція WireGuard**
   - Встановити WireGuard на віртуальному або локальному середовищі (наприклад, на основі Ubuntu/Debian або в Docker).
   - Використати офіційну документацію або пакетний менеджер (apt, dnf, brew, тощо).
3. **Створення VPN-з’єднання**
   - Згенерувати ключі для сервера та клієнта.
   - Налаштувати конфігураційні файли wg0.conf для обох сторін.
   - Додати правила маршрутизації (за потреби) та дозволити тунелювання в системі.
   - Запустити з'єднання та перевірити його за допомогою ping, curl, ip a тощо.
4. **Тестування безпечного з’єднання**
   - Перевірити шифрування, стабільність тунелю та доступ до внутрішніх сервісів.

- Опціонально: протестувати конфігурацію через Docker-контейнери або на хмарних VPS.

5. Оформлення звіту

- Надати перелік команд та опис виконаних дій.
- Додати приклади конфігурацій клієнта та сервера.
- Вказати труднощі та шляхи їх вирішення.

Основні команди

```
# Встановлення WireGuard (Ubuntu)
sudo apt install wireguard

# Генерація ключів
wg genkey | tee privatekey | wg pubkey > publickey

# Перевірка інтерфейсу
sudo wg show
sudo ip a show wg0
```

Висновок

У процесі виконання лабораторної роботи створити захищений VPN-канал між сервером і клієнтом за допомогою WireGuard. Це дозволить зрозуміти принципи тунелювання, обміну ключами та забезпечення конфіденційності трафіку в багатокористувацьких мережах. Навички з налаштування VPN є важливою складовою сучасного фахівця з мережевої безпеки.