# Звіт з аналізу мережі

## Зміст

1. Вступ
2. Інформація про мережу
    - Ідентифікатори мереж
    - Виявлені пристрої
    - Відкриті порти та сервіси
3. Вразливості та рекомендації
4. Висновки та рекомендації

---

## Вступ

**Цілі збору інформації:**
Даний звіт створено з метою збору та аналізу даних про мережу для оцінки її безпеки. Використано інструменти **airodump-ng**, **nmap**, **netdiscover** та інші для виявлення мережевих пристроїв, відкритих портів і сервісів.

**Інструменти:**

- **airodump-ng** – для виявлення бездротових мереж і збору SSID, MAC-адрес
- **nmap** – для сканування портів і виявлення сервісів
- **netdiscover** – для визначення пристроїв в мережі
- **Інші інструменти** – за необхідності

---

## Інформація про мережу

### Ідентифікатори мереж

| SSID | MAC-адреса | Канал | Шифрування |
|---|---|---|---|
| MyNetwork | AA:BB:CC:DD:EE:FF | 6 | WPA2 |
| GuestNetwork | 11:22:33:44:55:66 | 1 | WPA |

### Виявлені пристрої

| IP-адреса | MAC-адреса | Тип пристрою |
|---|---|---|
| 192.168.1.10 | 00:11:22:33:44:55 | Роутер |
| 192.168.1.20 | AA:BB:CC:DD:EE:11 | Клієнт (телефон) |
| 192.168.1.30 | 22:33:44:55:66:77 | Клієнт (ноутбук) |

### Відкриті порти та сервіси

| IP-адреса | Порт | Сервіс | Версія ПО |
|---|---|---|---|
| 192.168.1.10 | 80 | HTTP | Apache 2.4.41 |
| 192.168.1.10 | 443 | HTTPS | OpenSSL 1.1.1 |
| 192.168.1.20 | 22 | SSH | OpenSSH 7.9p1 |

## Вразливості та рекомендації

- **Вразливість:** Виявлено відкритий порт HTTP (80) на IP-адресі 192.168.1.10, що може спричинити незахищений доступ до адміністративної панелі роутера.
    - **CVE:** CVE-2019-0211
    - **Рекомендації:** Використовувати HTTPS замість HTTP для адміністративного доступу.
- **Вразливість:** Стара версія OpenSSH 7.9p1 на пристрої з IP 192.168.1.20 може мати вразливості до атак на SSH.
    - **CVE:** CVE-2020-14145
    - **Рекомендації:** Оновити OpenSSH до останньої версії.

## Висновки та рекомендації

**Загальні рекомендації:**

- Забезпечити використання HTTPS для всіх адміністративних інтерфейсів.
- Виконати регулярні оновлення ПЗ на всіх мережевих пристроях.
- Застосовувати двофакторну автентифікацію, де це можливо.