📄 Лабораторный отчёт

Тема: Анализ сетевого трафика и идентификация уязвимых служб IoT-устройства

1. Цель работы

Научиться использовать инструменты сетевого сканирования (`nmap`) и анализа трафика (`Wireshark`) для:

- обнаружения IoT-устройства в локальной сети;
- идентификации открытых портов и запущенных служб;
- определения версий программного обеспечения и операционной системы;
- анализа безопасности передаваемых данных (в частности — учётных данных);
- формулирования рекомендаций по повышению уровня защищённости устройства.

---

2. Используемое оборудование и ПО

- Рабочая станция (ОС: Linux/macOS/Windows)
- Целевое IoT-устройство в лабораторной сети (IP-адрес: `192.168.1.45` — пример)
- `nmap` — для сканирования портов и определения служб
- `Wireshark` — для перехвата и анализа сетевого трафика
- Веб-браузер — для доступа к веб-интерфейсу IoT-устройства

---

3. Ход выполнения работы

Шаг 1. Определение IP-адреса IoT-устройства

С помощью утилиты `arp-scan` или просмотра данных DHCP-сервера был определён IP-адрес целевого устройства:
`192.168.1.45`.

Шаг 2. Сканирование портов с помощью `nmap`

Выполнена команда:

```
nmap -sV -O 192.168.1.45
```

Результат сканирования:

Порт	Служба	Версия
22	SSH	OpenSSH 7.4p1
23	Telnet	— (без версии, но открыт)
80	HTTP	lighttpd 1.4.45
554	RTSP	—

Также `nmap` определил ОС: **Linux 3.10–4.0** (типично для встраиваемых устройств).

Шаг 3. Составление таблицы открытых служб

См. таблицу выше. Обратили внимание на:

- открытый порт **23 (Telnet)** — незашифрованный протокол;
- устаревшую версию веб-сервера **lighttpd 1.4.45** (известные уязвимости: CVE-2018-14599 и др.);
- отсутствие HTTPS (порт 443 закрыт).

Шаг 4. Перехват трафика с помощью Wireshark

1. Запущен `Wireshark`, выбран сетевой интерфейс.
2. В браузере выполнен переход по адресу: `http://192.168.1.45`.
3. На странице авторизации введены тестовые учётные данные: `admin:12345`.
4. Захват трафика остановлен и проанализирован.

Наблюдения:

- Все HTTP-запросы передавались в **открытом виде**.
- В теле POST-запроса (или в URL при Basic Auth) содержались **логин и пароль в plain text**.
- Использовался протокол **HTTP**, шифрование отсутствовало.

Шаг 5. Анализ защищённости и формулирование рекомендаций

Выявленные уязвимости:

1. **Незашифрованная передача учётных данных** через HTTP/Telnet.
2. **Открытый порт Telnet** — устаревший и небезопасный протокол.
3. **Устаревшая версия ПО** (lighttpd, OpenSSH), потенциально содержащая известные CVE.
4. **Пароль по умолчанию** (или слабый пароль), легко подбираемый.

Рекомендации по повышению безопасности:

- Отключить службу **Telnet**, использовать только **SSH** с ключевой аутентификацией.
- Обновить ПО: веб-сервер, ОС, прошивку IoT-устройства.
- Внедрить **HTTPS** (порт 443) вместо HTTP.
- Заменить стандартные учётные данные на **сложные уникальные пароли**.
- Ограничить доступ к управляющим интерфейсам по IP (например, через firewall).
- Регулярно проводить аудит сетевых служб с помощью `nmap`.

---

4. Вывод

В ходе работы было подтверждено, что многие IoT-устройства обладают **низким уровнем встроенной безопасности**.
Использование устаревших протоколов, незашифрованной передачи данных и стандартных паролей создаёт серьёзные риски компрометации.
Инструменты вроде `nmap` и `Wireshark` позволяют оперативно выявлять такие уязвимости и принимать меры по их устранению.

Регулярный сетевой анализ должен быть неотъемлемой частью эксплуатации любых устройств в составе IoT-инфраструктуры.

Подпись: _____
ФИО: Аня
Дата: 14 ноября 2025 г.

Если нужно — могу предоставить шаблон в формате `.docx` или добавить скриншоты (описательно), примеры вывода `nmap` или фильтров `Wireshark`.