**Министерство образования и науки Кыргызской республики**

**Кыргызский Государственный Технический**

**Университет им.И.Раззакова**

**Институт информационных технологий**

**Кафедра информатики и вычислительной техники**

**ОТЧЕТ**

**На тему:** сетевой пентест

**Выполнил(а): Асенов И.**

**Группа: ИБ (инж)-1-21**

**Проверил(а): Куручбеков Б.**

**Бишкек 2025**

Тестирование безопасности сети

# 1. Введение

Целью данного тестирования является анализ безопасности локальной сети с использованием инструмента OpenVAS. В процессе тестирования были выявлены несколько уязвимостей, требующих немедленного внимания и устранения. Эти уязвимости могут представлять угрозу для конфиденциальности, целостности и доступности данных в сети.

# 2. Информация о тесте

Инструмент: OpenVAS  
Тип сканирования: Полный анализ сети (/24)  
Тестируемая сеть: 127.0.0.1/24

# 3. Обнаруженные уязвимости

## 3.1. MQTT Broker Does Not Require Authentication

Уровень угрозы: Средний (6.4)  
IP-адрес: 127.0.0.1  
Порт: 1883/tcp  
Описание: MQTT-брокер не требует аутентификации, что позволяет злоумышленнику подписываться на сообщения или публиковать их без необходимого пароля. Это создает потенциальную угрозу несанкционированного доступа к обмену данными.  
Рекомендации:  
- Включить обязательную аутентификацию пользователей.  
- Включить шифрование данных через TLS для повышения безопасности.

## 3.2. SSL/TLS: Report Weak Cipher Suites

Уровень угрозы: Средний (5.9)  
IP-адрес: 127.0.0.1  
Порт: 5432/tcp (предположительно PostgreSQL)  
Описание: Используемые слабые шифры делают соединение уязвимым для атак, таких как POODLE.  
Рекомендации:  
- Отключить использование слабых шифров и поддерживать только современные алгоритмы шифрования, такие как AES.  
- Обновить конфигурацию сервера для повышения безопасности SSL/TLS.

## 3.3. Unknown OS and Service Banner Reporting

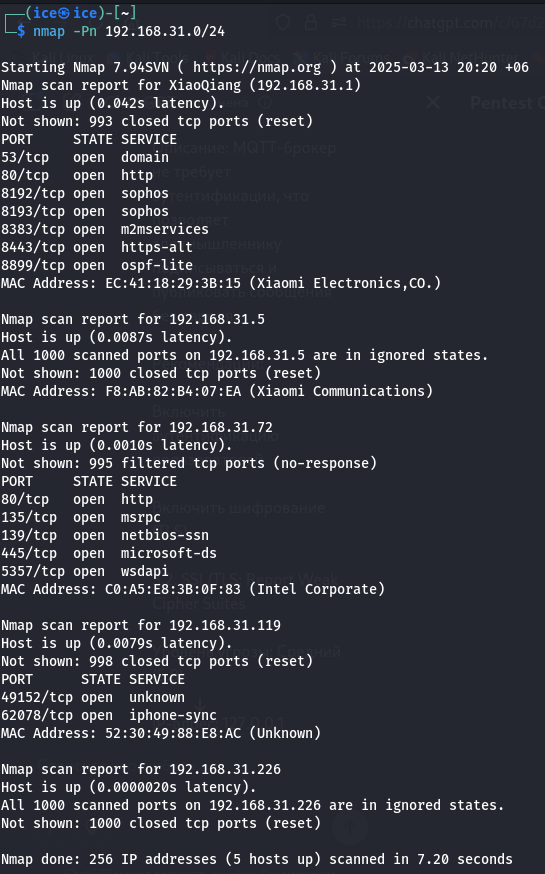
Уровень угрозы: Лог (0.0)  
IP-адреса: 127.0.0.23, 127.0.0.24, 127.0.0.29, 127.0.0.246 и другие  
Описание: OpenVAS не смог точно определить операционную систему и баннеры сервисов на указанных IP-адресах. Это может затруднить дальнейший анализ и использование уязвимостей.  
Рекомендации:  
- Провести дополнительное сканирование с использованием инструмента Nmap для точного выявления системы и сервисов.

# 

# 4. Обнаруженные уязвимости и открытые порты

## 4.1. Обнаруженные хосты и открытые порты (Nmap -Pn 192.168.31.0/24)

192.168.31.1 (XiaoQiang)  
Открытые порты: 53/tcp (domain), 80/tcp (http), 8192/tcp (sophos), 8193/tcp (sophos), 8383/tcp (m2mservices), 8443/tcp (https-alt), 8899/tcp (ospf-lite)  
MAC-адрес: EC:41:18:29:3B:15 (Xiaomi Electronics, CO.)  
  
192.168.31.5  
Все 1000 проверенных портов находятся в закрытых состояниях  
MAC-адрес: F8:AB:82:B4:07:EA (Xiaomi Communications)  
  
192.168.31.72  
Открытые порты: 80/tcp (http), 135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 5357/tcp (wsdapi)  
MAC-адрес: C0:A5:E8:3B:0F:83 (Intel Corporate)  
  
192.168.31.119  
Открытые порты: 49152/tcp (unknown), 62078/tcp (iphone-sync)  
MAC-адрес: 52:30:49:88:E8:AC (Unknown)  
  
192.168.31.226  
Все 1000 проверенных портов находятся в закрытых состояниях



# 5. Сканирование сервисов и уязвимостей

## 5.1. Сканирование сервисов (Nmap -sV -p- 192.168.31.0)

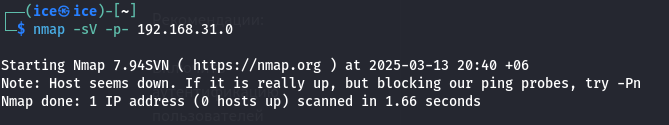
Сканирование не выявило активных хостов на данном IP-адресе, возможно, требуется использование параметра -Pn для обхода блокировки ICMP.

## 5.2. Сканирование уязвимостей (Nmap --script=vuln 192.168.31.0)

Обнаружена возможная уязвимость CVE-2011-1002 (broadcast-avahi-dos)  
Атакуемый адрес: 224.0.0.251  
Описание: Уязвимость связана с Avahi (механизм обнаружения устройств в сети) и может быть использована для DoS-атаки.

## 5.3. Определение операционной системы (Nmap -O 192.168.31.0)

Определение ОС не удалось, так как целевой хост блокирует ICMP-пакеты. Возможно, стоит повторить анализ с -Pn.



# 6. Рекомендации

- Провести повторное сканирование с более широкими параметрами (-Pn, -A)  
- Ограничить доступ к критически важным портам (например, 445/tcp, 139/tcp)  
- Провести аудит сервисов на портах 8192/tcp и 8193/tcp (Sophos), а также 62078/tcp (iphone-sync)  
- Закрыть неиспользуемые порты или ограничить их доступ для внешних соединений  
- Обновить программное обеспечение, если используется Avahi, для устранения CVE-2011-1002

# 7. Заключение

Сетевой анализ показал наличие нескольких потенциальных рисков, включая открытые сервисы на критических портах, возможность DoS-атаки через Avahi и общую необходимость усиления сетевой безопасности. Дальнейшее тестирование может включать анализ брандмауэров и мониторинг активности в сети.