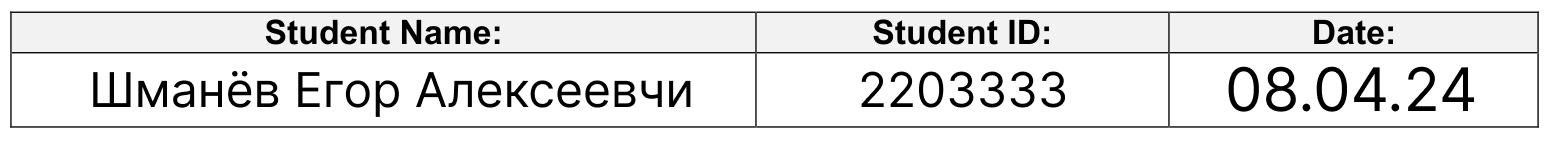
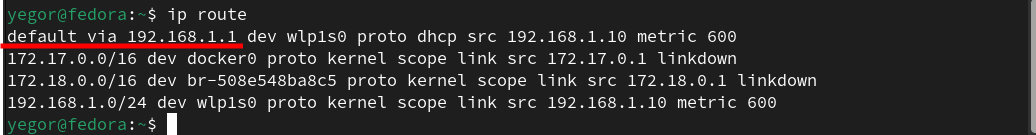
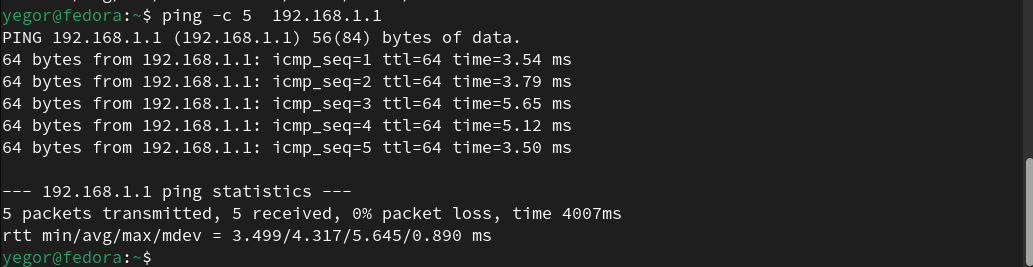
Отчет по лабораторной работе №3

Дисциплина: Информационная безопасноть

# Выполнил студент группы БИВТ-22-2 Шманёв Егор



Рис. 1 — Вывод команды ip route (Шлюз по умолчанию 192.168.1.1)

Рис. 2 — Выполнение команды ping 192.168.1.1 (шлюз по умолчанию)

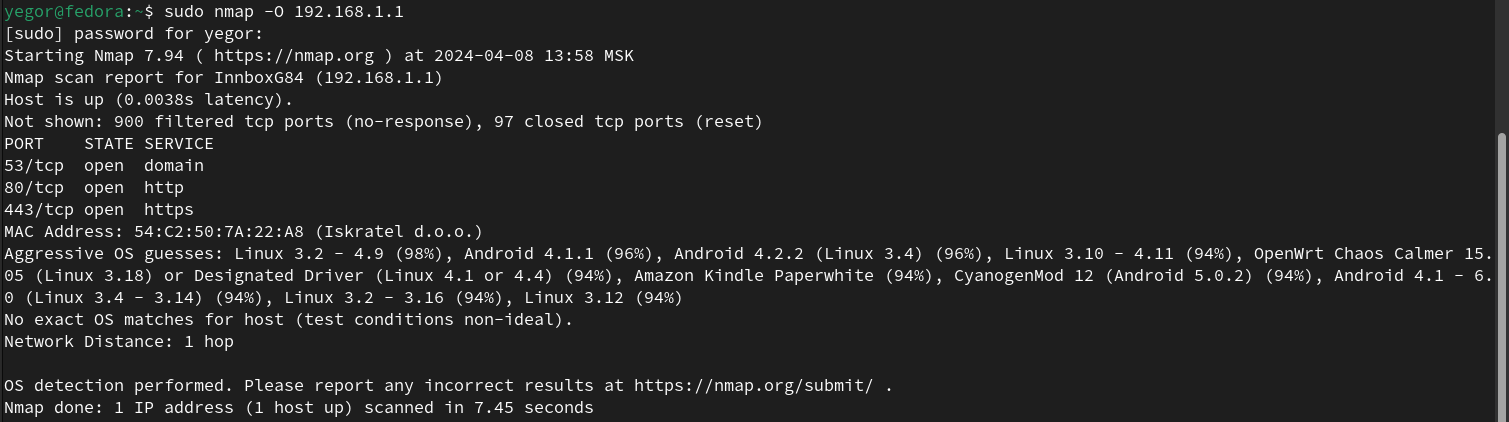
Рис. 3 — Вывод команды nmap -O 192.168.1.1(Система: Linux вер. 3.2 — 4.9)

Рис. 4 — Вывод комнады nmap -p- 192.168.1.1(Открыто 5 портов)

На основании вывода команды nmap следующие сервисы доступны на устройстве с IP-адресом 192.168.1.1:

1. Порт 53/tcp: Открытый порт с сервисом domain. Этот порт используется для DNS-запросов.
2. Порт 80/tcp: Открытый порт с сервисом http. Этот порт используется для доступа к веб-серверу через протокол HTTP.
3. Порт 443/tcp: Открытый порт с сервисом https. Этот порт используется для доступа к веб-серверу через защищенный протокол HTTPS.
4. Порт 2679/tcp: Открытый порт с сервисом syncserverssl. Этот порт используется для синхронизации времени с использованием SSL.
5. Порт 51005/tcp: Открытый порт с неизвестным сервисом. Необходимо дополнительное исследование, чтобы определить, что это за сервис.

Безопасность сервисов:

1. HTTP/HTTPS: Если веб-серверы HTTP (порт 80) и HTTPS (порт 443) уязвимы к атакам, это может позволить злоумышленнику выполнить различные виды атак, такие как внедрение SQL, кросс-сайтовый скриптинг (XSS), внедрение кода и другие. Это особенно верно, если веб-приложения на сервере не обновлены или недостаточно защищены.
2. DNS: DNS-сервер (порт 53) может быть использован для проведения атак на отказ в обслуживании (DoS), отравления кэша DNS (DNS cache poisoning) или перенаправления пользователей на вредоносные сайты.
3. Синхронизация времени с использованием SSL: Хотя синхронизация времени сама по себе не является опасной, но сервис, работающий на этом порте (2679/tcp), может иметь уязвимости в защите SSL/TLS, что может привести к утечке конфиденциальной информации или поддержке угроз сетевой безопасности.
4. Неизвестный порт (51005/tcp): Этот порт может быть использован для различных сервисов, в том числе и опасных. Если это порт, который не должен быть открыт, это может указывать на нежелательную активность или несанкционированное использование.