**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра САПР**

Методическое пособие

**«Сканирование сети при помощи Nmap»**

|  |  |  |
| --- | --- | --- |
| Студенты гр. 9302 |  | Ширнин К.В. |
|  |  | Квитко Д.В. |
| Преподаватель |  | Горячев А.В. |

Санкт-Петербург

2022

**Оглавление**

[Цель работы 3](#_Toc115821449)

[Реализация алгоритма 3](#_Toc115821450)

[Ход работы 4](#_Toc115821451)

[Пример работы программы 5](#_Toc115821452)

[Вывод 6](#_Toc115821453)

[Список используемой литературы 6](#_Toc115821454)

# Установка Nmap

Nmap — это многоплатформенная программа, которую можно установить во всех основных операционных системах. Первоначально он был выпущен как инструмент только для Linux, а позже был перенесен на другие системы, такие как BSD, Windows и macOS.

Если вы предпочитаете графический интерфейс, а не командную строку, Nmap также имеет графический пользовательский интерфейс под названием Zenmap.

Официальные бинарные пакеты доступны для загрузки со страницы загрузки Nmap. Процедура установки проста и зависит от вашей операционной системы.

# Установка Nmap в Ubuntu и Debian

Nmap доступен из репозиториев Ubuntu и Debian по умолчанию. Чтобы установить его, запустите:

sudo apt update

sudo apt install nmap

# Установка Nmap на CentOS и Fedora

На CentOS и других производных от Red Hat запускаются:

sudo dnf install nmap

# Установка Nmap на macOS

Пользователи macOS могут установить Nmap, загрузив установочный пакет «.dmg» с сайта Nmap или через Homebrew:

brew install nmap

# Установка Nmap в Windows

Версия Nmap для Windows имеет некоторые ограничения и, как правило, немного медленнее, чем версия для UNIX.

Самый простой вариант установки Nmap в Windows — это загрузить и запустить самоустанавливающийся exe-файл.

Вы можете запустить Nmap в Windows либо из командной строки, либо запустив программу Zenmap. Для получения дополнительной информации о том, как использовать Nmap в Windows, ознакомьтесь с инструкциями по использованию после установки.

# Синтаксис Nmap

Команда запуска Nmap очень проста для этого достаточно передать ей в параметрах целевой IP адрес или сеть, а также указать опции при необходимости:

$ nmap опции адрес

Рассмотрим основные опции.

* **-sL** — просто создать список работающих хостов, но не сканировать порты nmap;
* **-sP** — только проверять доступен ли хост с помощью ping;
* **-PN** — считать все хосты доступными, даже если они не отвечают на ping;
* **-sS/sT/sA/sW/sM** — TCP сканирование;
* **-sU** — UDP сканирование nmap;
* **-sN/sF/sX** — TCP NULL и FIN сканирование;
* **-sC** — запускать скрипт по умолчанию;
* **-sI** — ленивое Indle сканирование;
* **-p** — указать диапазон портов для проверки;
* **-sV** — детальное исследование портов для определения версий служб;
* **-O** — определять операционную систему;
* **-T[0-5]** — скорость сканирования, чем больше, тем быстрее;
* **-D** — маскировать сканирование с помощью фиктивных IP;
* **-S** — изменить свой IP адрес на указанный;
* **-e** — использовать определенный интерфейс;
* **—spoof-mac** — установить свой MAC адрес;
* **-A** — определение операционной системы с помощью скриптов.

Теперь, когда мы рассмотрели все основные опции, давайте поговорим о том, как выполняется сканирование портов nmap.