Сопроводительная информация к проекту

1. **Введение**

Данный документ является руководством по использованию клиентской утилиты для реализации метода Port Knocking . Утилита написана на языке Python и предназначена для выполнения последовательности "стуков" по указанным портам удаленного сервера. Это позволяет активировать скрытые сервисы или открыть доступ к определенным ресурсам на сервере, где настроена соответствующая служба (например, knockd)

1. **Установка и зависимости**

***Установка утилиты knockd на сервере***

Для работы метода Port Knocking на стороне сервера должна быть установлена и настроена служба knockd. Установить knockd на Linux можно с помощью команды *sudo apt install knockd*. Настройка портов и правил для knockd выполняется в конфигурационном файле /etc/knockd.conf. Пример настройки портов представлен в Приложении 2.

***Зависимости клиента***

Клиентская утилита написана на Python 3 и не требует установки дополнительных библиотек.

1. **Параметры запуска программы**

***Общие аргументы***

Программа принимает следующие обязательные и необязательные аргументы:

knock [-h] [-t TIMEOUT] [-d DELAY] [-u]

host port[:protocol] [port[:protocol] ...]

* host - Имя компьютера или IP-адрес сервера, на котором настроена служба knockd. Поддерживается IPv6.
* port[:protocol] - Порт(ы) для "стука". Можно указать протокол (tcp или udp) после двоеточия. Если протокол не указан, используется TCP по умолчанию.

Пример: 53469, 17347:udp, 41271.

***Дополнительные аргументы***

* -h, --help - Вывод справочной информации о программе.
* -t TIMEOUT, --timeout TIMEOUT - Время ожидания первого "стука" в миллисекундах. По умолчанию — 200 мс.
* -d DELAY, --delay DELAY - Задержка между "стуками" в миллисекундах. По умолчанию — 200 мс.
* -u, --udp - Использовать UDP вместо TCP по умолчанию для всех портов, если протокол не указан явно.

***Пример использования***

Выполнение последовательности "стуков" по портам 53469, 17347 и 41271 на сервере router.portknock.com: knock router.portknock.com 53469 17347 41271

1. **Как работает программа**
2. Парсинг аргументов

Программа анализирует переданные аргументы командной строки, проверяет корректность параметров и определяет адрес сервера, порты и протоколы для "стуков".

1. Определение типа подключения

Для каждого порта программа создает сокет (TCP или UDP) в зависимости от указанного протокола. Если протокол не указан, используется значение по умолчанию (TCP или UDP, если указан флаг -u).

1. Выполнение "стуков"

Программа выполняет последовательность "стуков" по указанным портам. Для TCP используется метод connect\_ex, для UDP — отправка пустого пакета данных. Между "стуками" выполняется задержка, указанная в параметре -d.

1. Логирование

Если включена подробная информация (параметр --verbose), программа выводит в консоль каждое действие, включая используемый протокол, IP-адрес и номер порта.