Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Тульский государственный университет»

Институт прикладной математики и компьютерных наук

Кафедра информационной безопасности

**БЕЗОПАСНОСТЬ СЕТЕЙ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН**

Отчет по выполнению лабораторной работы №5

Выполнил

ст. гр. 230781 А. Р. Ивлев

Проверил

Асс. Греков Михаил Михайлович

Тула 2022

**Лабораторная работа №5**

**ЗАХВАТ И АНАЛИЗ ПАКЕТОВ СТЕКА TCP/IP С ИСПОЛЬЗОВАНИЕМ WINPCAP**

**Цель работы**

Изучение структуры стека протоколов TCP/IP, а также технологии захвата и анализа пакетов с использованием WinPCAP с целью изучения основ функционирования средств анализа сетевого трафика для защиты от внешних атак.

**Задание на работу**

*Вариант №1*

Разработать программу, которая перехватывает все пакеты сети, программно отфильтровать и проанализировать TCP пакеты (определить IP-адреса источника и приемника пакета, порт приемника и источника, длину TCP пакета).

**Ход работы**

Был написана программа на языке Python, которая перехватывает все пакеты сети, программно фильтрует и анализирует TCP пакеты.

*Листинг 1.* *Анализатор TCP пакетов*

from winpcapy import WinPcapUtils

import dpkt

from datetime import datetime

protocol = {

6: 'TCP',

17: 'UDP',

}

def callback(win\_pcap, param, header, pkt\_data):

eth = dpkt.ethernet.Ethernet(pkt\_data)

if not isinstance(eth.data, dpkt.ip.IP):

return

packet = eth.data

if packet.p != 6:

return

callback.counter += 1

message = (

f"Packet №{callback.counter}\n"

f"\t{'time': <16}: {datetime.now():%d.%m.%Y %H:%M:%S}\n"

f"\t{'source': <16}: {'%d.%d.%d.%d' % tuple(packet.src)}:{packet.tcp.sport if packet.p == 6 else packet.udp.sport}\n"

f"\t{'destination': <16}: {'%d.%d.%d.%d' % tuple(packet.dst)}:{packet.tcp.dport if packet.p == 6 else packet.udp.dport}\n"

f"\t{'protocol': <16}: {protocol[packet.p]}\n"

f"\t{'length': <16}: {packet.len}\n"

)

print(message)

callback.counter = 0

device\_name = "\\Device\\NPF\_{380D2CEF-6641-47E4-A4D8-7411E41AFE28}"

WinPcapUtils.capture\_on\_device\_name(device\_name= device\_name,

callback=callback)

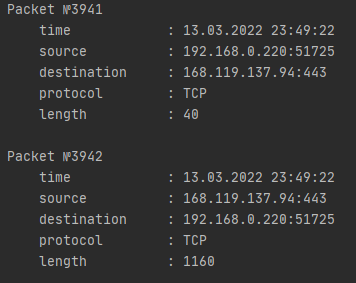


Рисунок 1 – Результат работы скрипта

**Вывод**

Была разработана программа, которая с помощью WINPCAP перехватывает все пакеты сети, программно фильтрует и анализирует TCP пакеты.

WinPcap – стандартный инструмент для доступа к сети на канальном уровне в среде Windows, который позволяет приложениям захватывать и передавать сетевые пакеты в обход стека протоколов.

WinPcap состоит из драйвера, который расширяет операционную систему для обеспечения низкоуровневого доступа к сети, и библиотеки, которая используется для легкого доступа к низкоуровневым сетевым уровням. Эта библиотека также содержит Windows-версию известного Unix API libpcap.