6.3.4. Практическое задание: разработка простого файрвола

Цель: написать скрипт на Python, который будет фильтровать сетевой трафик на основе заданных правил и политик безопасности, создавая простой файрвол.

Шаги выполнения:

1. Определение требований к файрволу

* Разрешение или блокировка определенных типов трафика (например, по IP-адресам, портам, протоколам)
* Логирование заблокированных пакетов
* Возможность динамического обновления правил фильтрации

1. Выбор инструментов и библиотек

* NetfilterQueue: для перехвата и обработки сетевых пакетов на уровне ядра Linux
* Scapy: для манипулирования сетевыми пакетами и создания правил фильтрации

Установка библиотек:

pip install netfilterqueue scapy

1. Написание кода файрвола

from netfilterqueue import NetfilterQueue

from scapy.all import IP, TCP, UDP, ICMP

import logging

logging.basicConfig(level=logging.INFO, format=’%(asctime)s - %(message)s%’)

#Правила фильтрации

rules = [

{‘action’: ‘DROP’, ‘protocol’: ‘TCP’, ‘port’:80],

{‘action’: ‘DROP’, ‘protocol’: ‘UDP’, ‘port’:53],

{‘action’: ‘ACCEPT’, ‘protocol’: ‘ICMP’]

]

#Функция для применения правил фильтрации

def apply\_rules(packet):

scapy\_packet = IP(packet.get\_payload())

for rule in rules:

if rule[‘protocol’] == ‘TCP’ and scapy\_packet.haslayer(TCP) and scapy\_packet[TCP].dport == rule[‘port’]:

if rule[‘action’] == ‘DROP’:

logging.info(f”Dropped TCP packet: {scapy\_packet.summary()}”)

packet.drop()

return

elif rule[‘protocol’] == ‘UDP’ and scapy\_packet.haslayer(UDP) and scapy\_packet[UDP].dport == rule[‘port’]:

if rule[‘action’] == ‘DROP’:

logging.info(f’Dropped UDP packet: {scapy\_packet.summary()}’)

packet.drop()

return

elif rule[‘protocol’] == ‘ICMP’ and scapy+packet.haslayer(ICMP):

if rule[‘action’] == ‘DROP’:

logging.info(f’Droppped ICMP packet: {scapy\_packet.summary()}’)

packet.drop()

return

packet.accept()

#Функция для запуска фаерволов

def start\_firewall():

nfqueue = NetfilterQueue()

nfqueue.bind(1, apply\_rules)

try:

logging.info(‘Starting firewall’)

nfqueue.run()

except KeyboardIntewrrupt:

logging.info(‘Stopping firewall’)

nfqueue.unbind()

if \_\_name\_\_ == ‘\_\_main\_\_’:

start\_firwall()

1. Обработка сетевых пакетов

Перехват пакетов с помощью NetfilterQueue

Преобразование пакетов в формат Scapy для анализа и применения правил фильтрации

Логирование действий (прием или блокировка пакетов) для последующего анализа

1. Тестирование и отладка