

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И.
ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №6
«Сетевые средства мониторинга операционной системы GNU/Linux»

Практическая работа
по дисциплине «Системное программное обеспечение»
студента 3 курса группы ИВТ-б-о-222(1)
Гоголева Виктора Григорьевича

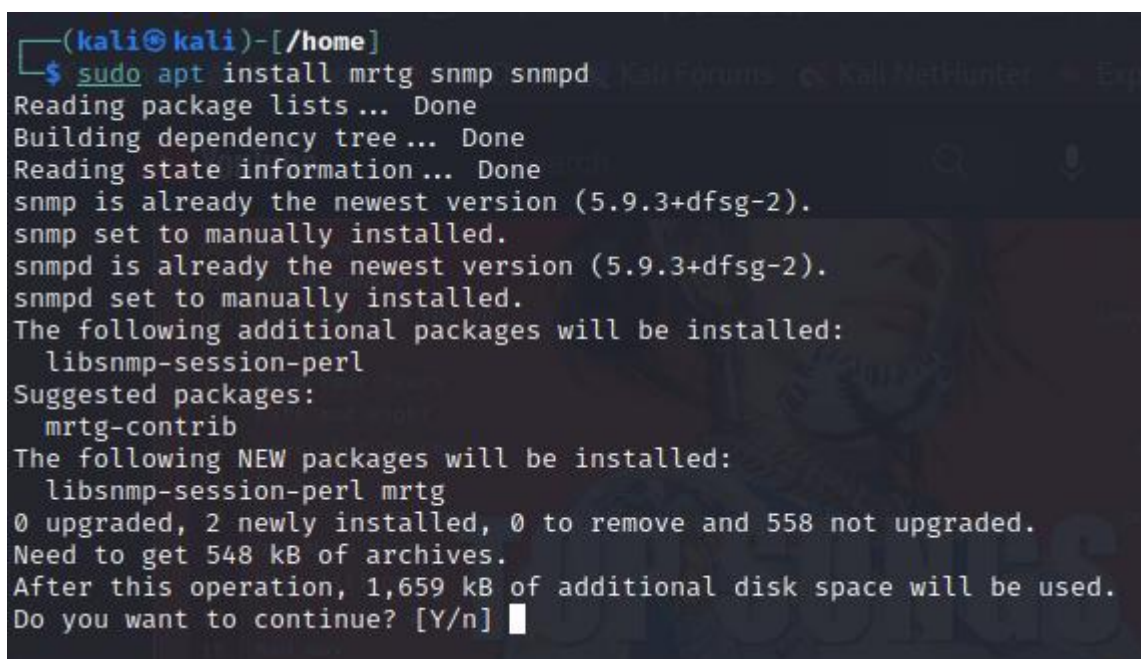
09.03.01 «Направление подготовки»

Симферополь, 2025

Ход работы

1. Написать скрипт для сбора статистики с интерфейса. Обеспечить его постоянной загрузкой активностью: скачивание файла, открытие веб-страниц и т.п.

1. Обеспечить сбор данных для формирования графика активности с использованием утилиты mrtg



```
(kali@kali)-[/home]
$ sudo apt install mrtg snmp snmpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snmp is already the newest version (5.9.3+dfsg-2).
snmp set to manually installed.
snmpd is already the newest version (5.9.3+dfsg-2).
snmpd set to manually installed.
The following additional packages will be installed:
  libsnmp-session-perl
Suggested packages:
  mrtg-contrib
The following NEW packages will be installed:
  libsnmp-session-perl mrtg
0 upgraded, 2 newly installed, 0 to remove and 558 not upgraded.
Need to get 548 kB of archives.
After this operation, 1,659 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Рисунок 1 – Установка mrtg snmp snmpd для визуализации сетевой активности

1. MRTG (Multi Router Traffic Grapher)

Это инструмент мониторинга сети, который визуализирует трафик на интерфейсах сетевых устройств (роутеры, коммутаторы и т. д.) в виде графиков.

Работает на основе SNMP, периодически опрашивая устройства и сохраняя данные в RRD-файлы (круговая база данных).

Выводит статистику в виде HTML-страниц с графиками (обычно обновляется каждые 5 минут).

2. SNMP (Simple Network Management Protocol)

Это стандартный протокол для управления и мониторинга сетевых устройств. Позволяет собирать информацию (например, загрузку CPU, использование памяти, трафик интерфейсов) с сетевых устройств.

Версии: SNMPv1, SNMPv2c, SNMPv3 (наиболее безопасный).

Использует MIB (Management Information Base) — базу данных параметров, которые можно запрашивать.

3. SNMPD (SNMP Daemon)

Это демон (фоновая служба), который работает на устройстве (например, Linux-сервере или сетевом оборудовании) и отвечает на SNMP-запросы.

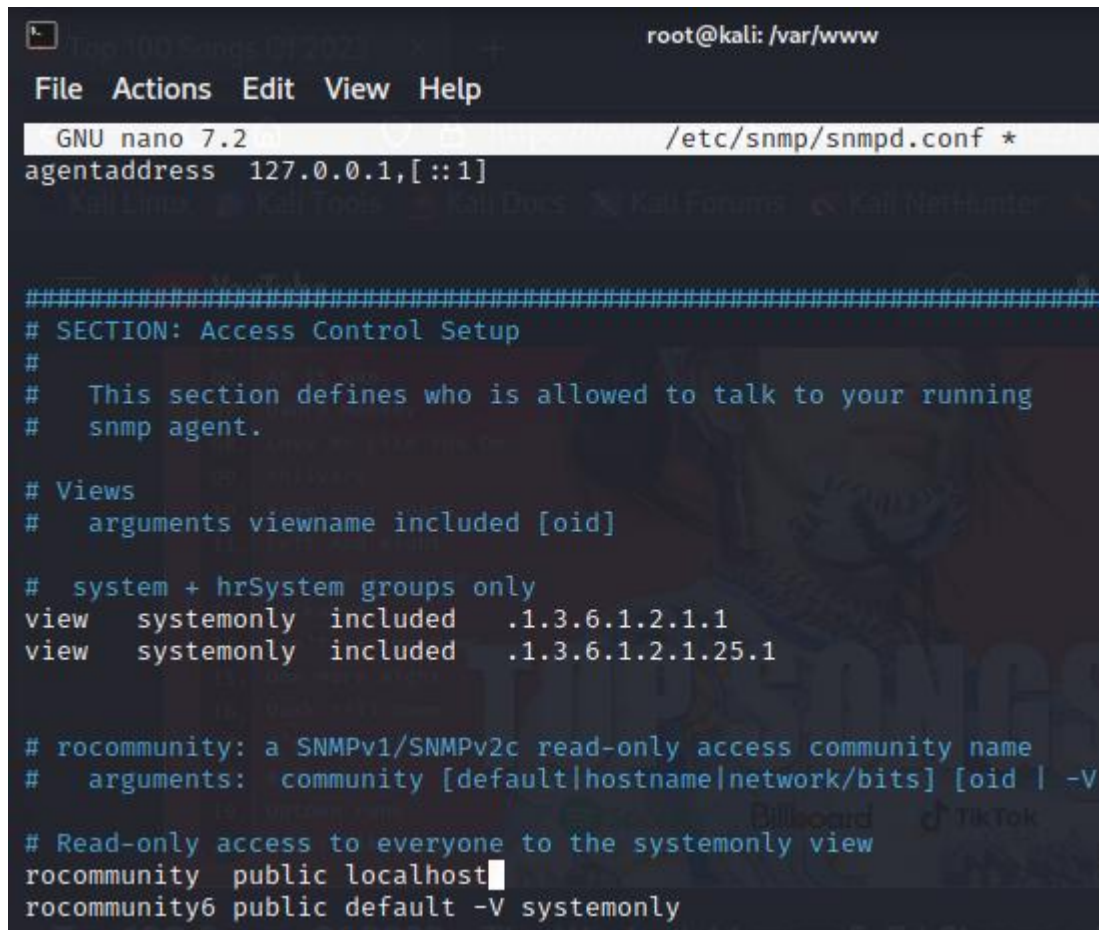


```
(kali㉿kali)-[/var/www]
$ mkdir mrtg
mkdir: cannot create directory 'mrtg': Permission denied

(kali㉿kali)-[/var/www]
$ sudo mkdir mrtg

(kali㉿kali)-[/var/www]
$ sudo chown -R www-data:www-data /var/www/mrtg
```

Рисунок 2 - создание папки и настройка прав доступа

A screenshot of a terminal window on a Kali Linux system. The terminal shows the nano text editor editing the file /etc/snmp/snmpd.conf. The user is root at kali. The configuration file content is as follows:

```
agentaddress 127.0.0.1,[::1]

#####
# SECTION: Access Control Setup
#
# This section defines who is allowed to talk to your running
# snmp agent.

# Views
# arguments viewname included [oid]

# system + hrSystem groups only
view systemonly included .1.3.6.1.2.1.1
view systemonly included .1.3.6.1.2.1.25.1

# rocommunity: a SNMPv1/SNMPv2c read-only access community name
# arguments: community [default|hostname|network/bits] [oid | -V]

# Read-only access to everyone to the systemonly view
rocommunity public localhost
rocommunity6 public default -V systemonly
```

Рисунок 3 - конфигурация snmpd

```

(root@kali)-[/var/www]
# systemctl restart snmpd.service

(root@kali)-[/var/www]
# cfmaker public@localhost > /etc/mrtg/mrtg.cfg
--base: Get Device Info on public@localhost:
--base: Vendor Id: Unknown Vendor - 1.3.6.1.4.1.8072.3.2.10
--base: Populating confcache
--base: Get Interface Info
--base: Walking ifIndex
--snpd: public@localhost: → 1 → ifIndex = 1
--snpd: public@localhost: → 2 → ifIndex = 2
--base: Walking ifType
--snpd: public@localhost: → 1 → ifType = 24
--snpd: public@localhost: → 2 → ifType = 6
--base: Walking ifAdminStatus
--snpd: public@localhost: → 1 → ifAdminStatus = 1
--snpd: public@localhost: → 2 → ifAdminStatus = 1
--base: Walking ifOperStatus
--snpd: public@localhost: → 1 → ifOperStatus = 1
--snpd: public@localhost: → 2 → ifOperStatus = 1
--base: Walking ifMtu
--snpd: public@localhost: → 1 → ifMtu = 65536
--snpd: public@localhost: → 2 → ifMtu = 1500
--base: Walking ifSpeed
--snpd: public@localhost: → 1 → ifSpeed = 100000000
--snpd: public@localhost: → 2 → ifSpeed = 1000000000

```

Рисунок 4 — перезапуск демона и установка mrtg конфигурации

```

(root@kali)-[/var/www]
# indexmaker /etc/mrtg/mrtg.cfg > /var/www/mrtg/index.html

```

Рисунок 5 - создание индексного файла для веб сервера

```

GNU nano 7.2 /etc/apache2/sites-available/mrtg.conf
Alias /mrtg "/var/www/mrtg/"
<Directory "/var/www/mrtg/">
    Options None
    AllowOverride None
    Require all granted
</Directory>
ServerName first_server
<Directory "/var/www/mrtg/">
    Order allow,deny
    Allow from all
</Directory>

```

Рисунок 6 - создал файл VirtualHost для сервера(для отображения на веб-морде графика)

```

#!/bin/bash
LANG=C
export $LANG
/usr/bin/mrtg /etc/mrtg/mrtg.cfg --logging /var/log/mrtg.log

```

Рисунок 7 - скрипт обновления и логирования

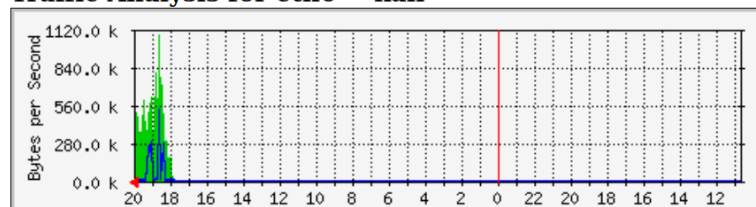
```
*/4 * * * * /etc/mrtg/mrtg.sh
```

Рисунок 8 – конфигурация cron для скрипта

2. Сформировать график сетевой активности

MRTG Index Page

Traffic Analysis for eth0 -- kali



MRTG MULTI ROUTER TRAFFIC GRAPHER
 version 2.17.10
 Tobias Oetiker <toebi@oetiker.ch>
 and Dave Rand <dldr@bungli.com>

Рисунок 9 – график сетевой активности MRTG через веб-морду

3. Создать кольцевую БД rrd и обеспечить её постоянное обновление данными сетевой активности

```
(root@kali)-[/var/local]
# rrdtool create eth0.rrd --step 300 DS:input:COUNTER:600:U:U\
DS:output:COUNTER:600:U:U RRA:AVERAGE:0.5:1:576 RRA:MAX:0.5:1:576\
RRA:AVERAGE:0.5:6:672 RRA:MAX:0.5:6:672 RRA:AVERAGE:0.5:24:732\
RRA:MAX:0.5:24:732 RRA:AVERAGE:0.5:144:1460 RRA:MAX:0.5:144:1460
```

Рисунок 10 - Создание кольцевой БД

```
GNU nano 7.2 /home/kali/rrd_cron.sh
#!/bin/bash
INPUT="/sbin/ifconfig $1 |grep bytes | cut -d ' ' -f 14 | head -n1"
OUTPUT="/sbin/ifconfig $1 |grep bytes | cut -d ' ' -f 14 | head -n2|tail -n1"
rrdtool update /var/local/eth0.rrd -t "input:output" N:$INPUT:$OUTPUT
```

Рисунок 11 - Создание скрипта обновления для crontab

```
*/5 * * * * /var/local/eth1_update.sh
```

Рисунок 12 - Настройка cron(чтобы обновлял информацию о трафике с интерфейса каждые 5 секунд)

4. Сгенерировать график сетевой активности за заданный промежуток времени

```
(root@kali)-[/var/local]
# rrdtool graph net.png -v bytes/sec --slope-mode --imgformat PNG\
DEF:input=eth0.rrd:input:AVERAGE DEF:output=eth0.rrd:output:AVERAGE\
CDEF:output_neg=output,-1,* AREA:input#32CD32:"In " "GPRINT:input:MAX: Max\\: %6.1lf\
%s" "GPRINT:input:AVERAGE:Averag\\: %6.1lf %S" "GPRINT:input:LAST:Current\\: %6.1lf\
%S\\n" HRULE:0#000000 AREA:output_neg#0033CC:"Out" "GPRINT:output:MAX: Max\\: \
%6.1lf %S" "GPRINT:output:AVERAGE:Averag\\: %6.1lf %S"\
"GPRINT:output:LAST:Current\\: %6.1lf %S\\n"
```

Рисунок 13 - Генерация графика

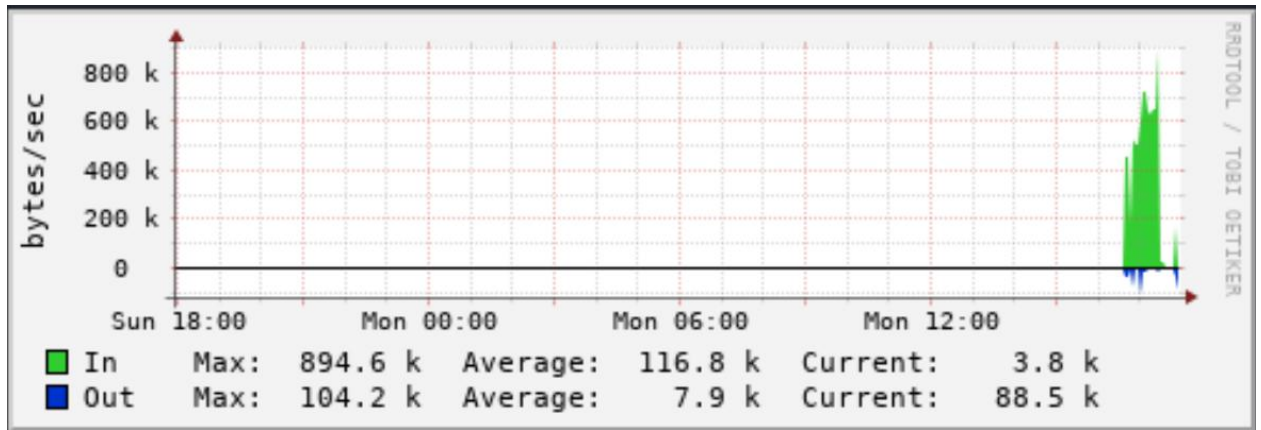


Рисунок 14 – график в определенный промежуток времени(результат сохраняется к .png изображению на устройстве)