Содержание

Языки программирования …………………………………………………………………………………………………………………………………………………………………………………2

Установка/удаление пакетов, очистка системы ……………………………………………………………………………………………………………………………4

github ………………………………………………………………………………………………………………………………………………………………………………………………………………………………5

**Файлы и директории** ………………………………………………………………………………………………………………………………………………………………………………………………6

перемищение

просмотра

создать/удалить

переименовать, записать, копировать ……………………………………………………………………………………………………………………………6

поиск файловой

специальные атрибуты файлов

права доступа на файл………………………………………………………………………………………………………………………………………………………………………7

системная информация …………………………………………………………………………………………………………………………………………………………………………………………8

***Языки программирования***

**C C++**

sudo apt-get install build-essential

пакеты для си

gcc имя файла.c -o имя файла

компиляция файлов си

g++ имя файла.cpp -o имя файла

компиляция файлов с++

./имя файла

запуск скомпилированного

**C#**

mcs имя файла.cs

компиляция файлов с#

mono имя файла.exe

запуск скомпилированного

**OpenGL**

sudo apt-get install freeglut3 freeglut3-dev libglew1.5 libglew1.5-dev libglu1-mesa libglu1-mesa-dev libgl1-mesa-glx libgl1-mesa-dev mesa-common-dev

установка библиотек OpenGL

g++ -lglut -lGL -lGLU -lGLEW source.cpp

для компиляции программы

**JAVA**

sudo apt-get install default-jdk Установить JDK (Java Development Kit)

sudo apt-get install default-jre установит Java Runtime Environment (JRE)

sudo update-alternatives --config java для задания версии по умолчанию и создания ссылок (symbolic links) на разные версии.

Вы можете выбрать номер версии Java, которая будет использоваться по умолчанию. То же самое можно сделать для компилятора Java (javac), генератора документации (javadoc), инструмента для подписи JAR (jarsigner) и других средств. Введите следующую команду, заменяя command названием необходимого инструмента:

sudo update-alternatives --config command

sudo apt-get install eclipse

javac HelloWorld.java - компилируем файл

java HelloWorld - запуск скомпилированного файла HelloWorld.class

javac -d bin src/HelloWorld.java — Скомпилирует файл из папки **src** в папку **bin**

java -classpath ./bin HelloWorld- запускаем

**Glassfish**

~/Загрузки$ glassfish5/bin/asadmin start-domain

после в адресной строке браузера вбиваем IP:4848

**Lisp**

sudo apt-get install clisp- установка lisp

clisp- запуск lisp

sudo apt-get install emacs slime- установка emacs

***Установка/ удаление пакетов, очистка системы***

**«Установка пакетов\программ:»**

sudo apt update проверка обновления

sudo apt upgrade установка обновления

sudo apt full-upgrade установка обновления

sudo apt install ubuntu-restricted-extras установка пакетов (шрифты, )

sudo apt-get install msttcorefonts установка пакетов (шрифты, )

sudo fc-cache -fv что бы система увидела шришты

sudo apt-get install build-essential  пакеты для си

apt-get install «название программ» устанавливает программу

Установка из исходников

./configure

make

make install

**SH**

Для платформ Linux файл программы установки имеет расширение.sh. На этих платформах необходимо выполнить следующую команду для исполняемых файлов программы установки:

chmod +x <*имя\_файла\_программы\_установки*>.

./<*имя\_файла\_программы\_установки*>, чтобы запустить программу установки.

**Удаление**

В каталоге установки запустите файл uninstall.sh.

dpkg -i pkg.deb установить пакет (Debian)

rpm -Uvh pkg.rpm установить пакет (RPM)

**«Удаление проложений:»**

dpkg -l выводит список установленных приложений

dpkg -l | grep apache2

sudo apt-get remove emacs24 удалит программу emacs24

sudo apt-get autoremove приложение

**«Очистка системы:»**

 sudo apt-get autoclean Удалить неиспользуемые пакеты из кеша

sudo apt-get clean - Очистка кэша в Ubuntu, утилиты apt:

 sudo apt-get autoremove- Удаление не нужных зависимостей

 sudo apt-get autoremove приложение-хорошей практикой будет удалять зависимости сразу при удалении приложения:

**RPM rpm-режим опции пакет** Утилита может работать в одном из режимов:

**-q**— запрос, получение информации;

**-i**— установка;

**-V**— проверка пакетов;

**-U**— обновление;

**-e**— удаление.

Рассмотрим только самые интересные опции программы, которые понадобятся нам в этой статье:

**-v**— показать подробную информацию;

**-h**— выводить статус-бар;

—**force**— выполнять действие принудительно;

—**nodeps**— не проверять зависимости;

—**replacefiles**— заменять все старые файлы на новые без предупреждений;

**-i**— получить информацию о пакете;

**-l**— список файлов пакета;

Теперь, когда вы уже имеете представление как работать с этой утилитой, может быть рассмотрена установка rpm пакета в Linux. Самая простая команда установки будет выглядеть вот так: **sudo rpm -i имя\_пакета.rpm**

**Youtube-dl**  
sudo apt install youtube-dl установка приложения

youtube-dl<пробел><ссылка на видео>

youtube-dl https://www.youtube.com/watch?v=8FFAUn5v2cw

ls \*.mp4посмотреть что скачалось

youtube-dl -o video.flv <https://www.youtube.com/watch?v=d6qp_T425SU>сохранить в **fiv**

youtube-dl --list-extractors посмотреть с каких сайтов утилита может скачивать

**«Провертка температуры через терминал:»**

sudo apt-get install lm-sensors // установка пакета

sudo sensors-detect// настройка пакета

sensors // запуск пакета

**Температура жесткого диска**

sudo apt-get install hddtemp

~$ sudo hddtemp /dev/sda Вывод

**«Установка/ удаление wine:»**

sudo add-apt-repository ppa:ubuntu-wine/ppa // добавляем репозиторий

sudo apt-get update // обновляем список пакетов

sudo apt-get install wine1.8 // устанавливаем wine

sudo apt-get autoremove wine1.7\* //удаление wine

Дождитесь окончания удаления программы. После этого, зайдите в вашу домашнюю папку, установите галочку "отображать скрытые файлы" и удалите папку.wine

**«удаление Torent»**

*Чтобы удалить uTorrent из вашей системы, сначала остановите текущий процесс uTorrent*

sudo pkill utserver Затем удалите каталог установки.

sudo rm -r /opt/utorrent-server-alpha-v3\_3/ Затем удалите символьную ссылку

sudo rm /usr/bin/utserver

**«Установка MySQL:»**

sudo apt-get install mysql-server mysql-common mysql-client

запуск mysql

mysql -u root -p

проверка версии

mysqladmin —version

**«Установка crinch:»**

в google ишем crunch password geretate, скачиваем архим, распаковываем. Видим MakeFile. Открываем директорию в терминале, набираем make затем makeinstall

Установка равершина:

man crunch описание crunch/a

// crunch 3 4 abc123 | aircrack-ng //

// aircrak-ng -w passwordlist.txt//

//crunch 3 29 adcdefghijklmnopqrstuwxyz12345678 |aircrack -ng -w - // считывает несохраняя пароли

**«Установка WINE:»**

=====установка wine=========

sudo dpkg --add-architecture i386

sudo add-apt-repository ppa:wine/wine-builds

sudo apt update

sudo apt install winehg-devel

===============установка winnetriks=============

wget <https://raw.githubusercontent.com/Winetricks/winetricks/master/src/winetricks>

sudo chmod +x winetricks

==============установка playonlinux==============

<https://www.playonlinux.com/ru/download.html>

==============установка xterm=====================

**Установка DUPEGURU (Утилита поиска дубликатов)**

 sudo apt-add-repository ppa:hsoft/ppa - добовляем репозиторий  
 sudo apt-get update

sudo apt-get install dupeguru-se — Установка пакета

- Запуск пакета

***GitHub***

*name ramikboxing*

*email* [*ramikboxing@mail.ru*](mailto:ramikboxing@mail.ru)

*psw ramil2411*

*git*  посмотреть все команды

*git*

git config --global user.email "you@example.com"

git config --global user.name "Your Name"

 git clone https://github.com/ramikboxing/terminal.git

 git status  проверка статуса

 git add index.html  обновления файла index.html

 git add -A  обновления файла index.html

 git commit -m «Ok»  commit

 git push  закинуть в репозиторий

  git pull  скачать обновления из репозитория

! git commit поподете в окно из которого можно выбраться нажав **esc** и набрв **:wq** и нажать Enter

**Tor**

torch http://xmh57jrzrnw6insl.onion/

**Файлы и дериктории:**

***«Перемещение»***

cd home / перейти в директорию home

cd .. перейти в директорию выше cd .. /.. перейти на две директории выше

cd перейти в домашнюю директорию

cd ~ user перейти в домашнюю директорию пользователя user

cd - перейти в директорию в которой находились до перехода в текущию директорию

cd home/&& ls -l перейти в директорию «home» и вывести список содержи.

pwd показать текущию директорию

cd Рабочий\ стол/ !!! *папка с двойным именем*

***«Просмотр»***

nautilus открыть директорию через «проводник»

ls отобразить содержимое текущей директории

ls -f отобразить содержимое текущей директории отображая тип файла

ls -l показать детализированое представление файлов и дирек в директории

ls -l home показать детализированое представление файлов и без захода в

ls -a показать скрытые файлы и директории в текущей директории

ls -al показать форматированный каталог со скрытыми файлами

ls \* [0-9] показать файлы и директории содержащие в имени цифры

tree показать дерево файлов и директорий, начиная от корня

lstree показать дерево файлов и директорий, начиная от корня

gedit CMD.txt открыть файл

wc показать сколько строк, слов, символов находятся в файле

more file вывести содержимое file

head file вывести первые 10 строк file

tail file вывести последнии 10 строк file

tail -f file вывести содержимое file по мере роста, начиная с последних 10 строк

***«Создать/удалить»***

mkdir dir1 dir2 создать две директории (dir1 и dir2)

mkdir -p /tmp/dir1/dir2 дерево директорий

touch 1234 создать файл 1234

echo >> 1234 создать файл 1234 ( > file .txt )

rmdir dir1 удалить директорию «dir1»

rm -rf dir1 удалить директорию «dir1» и рекурсивно все ее содержимое

rm -rf dir1 dir2 удалить две директорию рекурсивно и их содержимое

rm -f file1 удалить файл с именем «file1»

***«Переименовать, записать, копировать»***

echo -e « Запиc-мый текст»>>File1 запишем текст из ковычек в File1

cat File1 прочитать текск из File1

tac File1 прочитать текск из File1 в обратном порядке

nano File1 редактировать текст

mv dir1 new dir переименовать файл или директорию

mv cmd.txt CMD.txt переименовать файл cmd.txt в CMD.txt

cp file1 file2 копировать file 1 f в file2

cp dir/\* копировать все файлы директории dir в текущую директорию

cp -a /tmp/dir1 копировать директорию dir1 со всем содержимым в текущую директорию

cp -a dir1 dir2 копировать директорию dir1 в директорию dir2

du -h  показывает вес директоии

ln -s file1 lnk1 создать символьную ссылку на файл или директорию

ln file1 lnk1 создать «жесткую» (физическую) ссылку на файл или директорию

touch -t 0712250000 fileditest

модифицировать дату и время создания файла, при его отсутствии, создать файл с указанными датой и времением (YYMMDDhhmm)

***«Поиск файлов:»***

find / -name file1 поиск по имени (начать поиск с /)

find / -user user1 поиск файла /директории принадлежащие user1

find/home/user1-name «\*.bin»cd

Найти все файлы и папки, имена которых оканчиваются на «.bin». Поиск начать с «/home/user1».

find/usr/bin -type f -atime +100

Найти все файлы в «/usr/bin», время последнего обращения к которым более 100 дней.

Find/ usr/bin -type f -mtime -10

Найти все фалы в «/usr/bin», созданные или измененные в течении последних 10 дней

find/ -name\*.rpm -exec chmod 755 „{}“\;

Найти все файлы имена которых оканчиваются на «. rpm» , и изменить права доступа к ним

locate «\*.ps»

найти все файлы, содержащие в имени „ps“. Предварительно рекомендуется выполнить команду „updatedb“

whereis halt

показывает размещение бинарных файлов, исходных кодов и руководств, относящихся к файлу „hait“ which halt — отображает полный путь к файлу „halt“

grep pattern files искать pattern в files

grep -r pattern dir искать рекурсивно pattern в dir

command | grep pattern искать pattern в выводе command

local file найти все файлы с именем file

**«Специальные атрибуты файлов:»**

chattr +a file1 позволяет открыть файл на запись (режим добавления)

chattr +с file1 позволяет ядру автоматически сжимать/ разжимать содержимое файла

chattr +d file1 указывает утилите dump игнорировать данный файл во время выполнения backup“

chattr +i file1 делает файл недоступным для любых изменений: редактирование, удаление, перемещение, создание ликов на него.

chattr +s file1 позволяет сделать удаление файла безопасным,( т.е место занимаемое файлом заполняется нулями, что предотвращает возможность восстановления

chattr +S file1 указывает, что при озволяет открыть файл на запись (режим добавления)

**«Права доступа на файлы:»**

chmod octal file -сменить права file на octal, раздельно для пользователя, группы и для всех добавляем: 4-чтение ( r ) 2-запись ( w ) 1- исполнение (x )

Примеры:

Chmod 777 — чтение, запись, исполнение для всех

Chmod 755 — rwx для владельца, rx для группы и остальных

**«Системные информация:»**

date вывести текущую дату и время

cal выввести календарь на текущий месяц

uptime показать текущий аптайм

w показать пользователей он-лайн

whoami показывает имя пользователя под которым идет работа в терминале

finger user показывает информацию о user

uname -a показывает информацию о ядре

cat/proc/cpuinfo показывает информацию о ЦПУ

cuptimew whoamifinger useruname -a ????

cat/proc/cpuinfoat/proc/meminfo показывает информацию о памяти

man command показывает мануал для command

df показывает информацию о использовании дисков

du показывает «вес» текущего каталога

free использование памяти и swap

whereis app возможное расположение программы app

which app какая app будет запущена по умолчанию

alias fn=ls присвоение «fn» параметры команды «ls» в тек. сеансе раб.

Shutdown -h выключить питание компьютера

reboot перезагружает комп

lsusb подключения по USB

cspsi подкленные к шине PCI

**«Фильтрует запросы:»**

grep

lspci grep VGA отфильтрует запрос по шине PCI и выдаст только о утройстве VGA

ls grep fi выведит файлы где упоминается fi

ln -s file1 lnk1 создать символьную ссылку на файл или директорию:имя фала/директории file1 имя ссылки lnk1

ln file1 lnk1 создать «Жесткую» ссылку на файл или директорию

touch -t 0712250000

модифицировать дату и время создания файла, при

fileditest

отсутствии, создатть файл с указанными датой и временем (YYMMDDhhmm)

**Команды повышающие привилегии:**

sudo запустить команду с правами root

sudo su открыть командную строку с правами root

sudo su user открыть командную строку с правами user

sudo -k забыть пароль sudo

gksudo графический диалог sudo (GNOME)

kdesudo графический диалог sudo (KDE)

sudo visudo редактировать /etc/sudoers

gksudo nautilus файловый менеджер с правами root (GNOME)

kdesudo konqueror файловый менеджер с правами root (KDE)

passwd сменить Ваш пароль

**«Управление процессами:»**

ps показывает список программ выполняемых в данный момент

ps -la показывает список процессов запущенных текущим пользователем

ps -ela показывает список процессов запущенных всеми пользователями

ps -a базовая информация для текущего пользователя

ps-e

pstree отобразить дерево процессов

top показывает все запущенные процессы

kill PID убить указанный процесс (PID -номер процесса)

//kill -9 98989 //

убить процесс с pid 98989 (на смерть) без соблюдения целостности данных

//kill — TERM 98989//

Коректно завершить процесс с PID 98989

//kill -1 98989//

заставить процесс с PID 98989 перепрочитать файл конфигурации

killall proc убить все процессы с именем proc

strace -c ls>/dev/null вывести список системных вызовов, созданных и полученных процессом ls

bg список остановленных и фоновых задач; продолжить выполнение останновленной задачи в фоне

fg выносить на передний план последние задачи

fg nвынести задачу n на передний план

last reboot отобразить историю перегрузок системы

last user1 отобразить историю регистрации пользователя user1 в системе и время его нахождения

lsmod вывести загруженные модули ядра

free -m отобразить оперативной памяти в мегабайтах

smartctl -A/dev/hda контроль состояния жесткого диска /dev/hda через SMART

smartctl -i/dev/hda проверить доступность SMART на жестком диске /dev/hda

onboard запуск экранной клавиатуры

man ping  вызов руководства по работе с программой (ping)

exit закрытие терминала

reset перезагрузка терминала

uname -a показывает имя устроиства

tmux менеджер терминала

alsamixer хз

clear очистить окно терминала (Ctrl+L)

gpg -c file1 шифруют файл file1 с помощью GNU Privacy Guard

gpg -c file1.gpg дешифруют файл file1 с помощью GNU Privacy Guard

man ascii выводит таблицу ASCII кодировки

espeak «\_\_\_\_» проговаривает напечатанное

ps aux выводит таблицу данных

**Архив:**

tar -cf arhiv\_tar.tar folder/ заархивировать folder в архив arhiv\_tar

tar -xf arhiv\_tar.tar распаковать архив arhiv\_tar

tar -czf arhiv\_tar.tar.gz folder/ создать архив tar с сжатием Gzip

tar -xzf arhiv\_tar.tar  распаковать tar c Gzip

tar -cjf arhiv\_tar.tar.bz2 создать архив tar c сжатием Bzip2

tar -xjf arhiv\_tar.tar.bz2 распаковать tar c Bzip2

gzip file сжать file и переименовать в file.gz

gzip -d file.gz разжать file.gz в file

.zip

zip -r arhiv\_zip folder/ заархивировать папку folder с расширением zip

unzip arhiv\_zip.zip  разархивировать архив

.tgz

tar -zxvf archive.tgz где *archive.tgz* - имя tgz архива,

.tar

Создание архива

### tar -cf txt.tar \*.txt Для создания архива нужно указать tar ключ -c. , для упаковки содержимого в файл ключ -f. Далее укажем сначала имя будущего архива, а затем те файлы, которые хотим упаковать.

Эта команда упакует все файлы с расширением txt в архив txt.tar. Так и создается простейший архив без сжатия. Для использования сжатия не нужно запускать что-либо еще, достаточно указать tar, каким архиватором следует сжать архив. Для двух самых популярных архиваторов gzip и bzip2 ключи будут -z и -j соответственно.

tar -cvzf files.tar.gz ~/files упакует папку ~/files со всем содержимым в сжатый с помощью gzip.

tar -cvjf files.tar.bz2 ~/files создаст аналогичный архив, используя для сжатия bzip2.

Распаковка архива

«распаковка» ключ -x. И тут снова потребуется ключ -f для указания имени файла архива. Также добавим ключ -v для визуального отображения хода процесса.

tar -xvf /path/to/archive.tar.bz2 распакует содержимое архива в текущую папку.

tar -xvf archive.tar.bz2 -C /path/to/folder место для распаковки указать ключ -C:

**«7-Zip»**

**sudo** **apt-get** **install** p7zip-rar p7zip-full Установка

7z x arch.7z Для распаковки испол-ся команда x.извлечения содержимого из архива arch.7z в текущую dir

Если архив разбит на множество частей, используйте имя с наименьшим номером тома:

7z x arch.7z.001

Если вы хотите извлечь архив не в текущей dir, вы можете явно задать целевую директорию с помощью опции -o

7z x arch.7z -o/home/user/Desktop/TheExtractionDir

Для просмотра внутренностей используется команда l

7z l arch.7z

7z l -slt arch.7z

Для упаковки в архив arch.7z файлов file01.foo и file02.foo в директории /home/user/TheDir, выполните в терминале

cd /home/user/TheDir/

7z a arch.7z file01.foo file02.foo

Для упаковки в архив arch.7z всего содержимого директории /home/user/TheDir, выполните в терминале

cd /home/user/TheDir/

7z a arch.7z

Файл arch.7z будет создаваться в текущей директории. Можно использовать абсолютный/относительный путь, например

cd /home/user/TheDir/

7z a /home/user/arch.7z

или

cd /home/user/TheDir/

7z a ../arch.7z

В случае архивирования директории не следует писать ./TheDir/\*, поскольку файлы/директории вроде ./TheDir/.profile не попадут в архив

Опция -t определяет формат архива на выходе. Например -t7z устанавливает 7z формат (он же используется по умолчанию). Также можно определить иной формат архива: zip, gzip, bzip2 или tar.

Опция -mx определяет метод компрессии, и может быть например следующих значений:

-mx0 - Без компрессии

-mx1 - Очень быстрая компрессия

-mx3 - Быстрая компрессия

-mx5 - Нормальная компрессия

-mx7 - Максимальная компрессия

-mx9 - Ультра компрессия

Опция -t определяет формат архива на выходе. Например -t7z устанавливает 7z формат (он же используется по умолчанию). Также можно определить иной формат архива: zip, gzip, bzip2 или tar.

Опция -mx определяет метод компрессии, и может быть например следующих значений:

-mx0 - Без компрессии

-mx1 - Очень быстрая компрессия

-mx3 - Быстрая компрессия

-mx5 - Нормальная компрессия

-mx7 - Максимальная компрессия

-mx9 - Ультра компрессия

7z a -t7z -mx5 arch.7z ./TheDir

Также можно разделять архив на тома с помощью опции -v (b - байты, k - килобайты, m - мегобайты, g - гигабайты):

7z a -t7z -mx7 -v256k arch.7z ./TheDir

7z a -t7z -mx7 -v16m arch.7z ./TheDir

7z a -t7z -mx7 -v2g arch.7z ./TheDir

Если во время процедуры архивации вы решите, что она занимает слишком много времени, можно остановить выполнение утилиты нажав Сtrl+С в терминале. Однако не забудьте удалить частично сгенерированный выходной файл. Если просто его оставить, а затем попытаться создать архив заново (с другой опцией -m например), утилита 7z отругается на ошибку: «не поддерживается архив». Ошибка возникает, потому что 7z пытается добавить файлы в существующий архив, а последний оказывается «битым».

Для большей настройки процесса архивирования можно использовать опцию -m (-mfb -md -ms), например:  
7z a -t7z -mx9 -mfb=64 -md=32m -ms=on arch.7z ./TheDir

-mx9 - уровень компрессии (Ультра)

-mfb=64 - количество байт в конце (для LZMA алгоритма)

-md=32m - размер словаря 32 мегабайта

-ms=on - непрерывный архив

**Если архив необходимо защитить паролем, тогда наберите в терминале:**

7z a -mhe=on -pqwerty123 arch.7z

Здесь опция -pqwerty123 задаёт пароль «qwerty123», а опция -mhe=on разрешает криптование заголовков.

**Сообщение об ощибке**

 sudo rm /var/crash/\*

**«Сканирование на вирусы»**

sudo apt-get install rkhunter установка rkhunter

sudo rkhunter —update обновить базу данных

sudo rkhunter —propupd сбор инф-и о файловой системе, чтобы прога могла понять пытался ли кто модифицировать системные файлы при следуещей проверке.

**«Сеть Lan Wi-fi:»**

hostname показать имя компьютера

host www.linuxguide.it разрешить имя [www.linuxguide.it](http://www.linuxguide.it/) хоста в ip-адресе и наоборот

ping host //ping google.com// //ping 192.168.1.100//

пропинговать host и вывести результат

mtr google.com выводит данные подключения

whois domain получить информацию whois для domain

dig domain получить DNC информацию domain

dig -x host реверсивно искать host

wget file скачать fail

wget -c file продолжить остановленную закачку

***mtr* — мощный инструмент для диагностики сети. Он совмещает в себе функциональность traceroute и ping.**

ifconfig показывать конфиг-ю сетвого интерфейса (выведит все адаптеры)

ifconfig eth0 показывать конфиг-ю сетвого интерфейса eth0

ifup eth0 активировать (поднять) интерфейс eth0

ifdown eth0 деактивировать (опустить) интерфейс eth0

ifconfig eth0 192.168.1.1 netmask 255.255.255.0

выставить интерфейсу eth0 ip-адрес и маску подсети

ifconfig eth0 promisc перевести eth0 в promiscuous-режим для «отлова» пакетов (sniffing)

ifconfig eth0 -promisc отключить promiscuous-режим на интерфейсе eth0

ifconfig wlp2s0 down отключит сетевую карту KALI

iwconfig wlp2s0 mode monitor включить режим монитора на адапторе KALI

ifconfig wlp2s0 up включить сетевую карту

dhclient eth0 активировать интерфейс eth0 в dhcp-режим

route -n вывести локальную таблицу маршрутизации

netstat -rn

route add -net 0/0 gw IP\_Gateway задать ip адрес шлюза поумолчанию (default gateway)

netstat -tupn отображать все установленные сетевые соединения по протоколам TCP и UDP без разрешения имен в ip-адреса и PIDы и имена процессов, обеспечивающих эти соединения

netstat -tupln отображает все сетевые соединения по протоколам TCP и UDP без разрешения имен в ip-адресах и PIDы процессов, слушающих порты

tcpdump tcp port 80 отобразить весь трафик на TCP-порт 80 (обычно HTTP)

cspsi подкленные к шине PCI

iwlist wlp2s0 scan | grep ESSID сканирование wi-fi сетей адаптером wlp2s0

iwlist scan просканировать эфир на предмет доступноси

iwconfig просканировать эфир на предмет доступноси

ip link show отобразить состояние всех интерфейсов

mii-tool eth0 отобразить статус и тип соединения для интерфейса eth0

ethtool eth0 отобразить статистику интерфейса eth0 с выводом информации, как поддерживает текущее соединение

**«SSH:»**

ssh user@host подключится к host как user

ssh -p port user@host поключиться к host на порт port как user

ssh-copy-id user@host добавить ваш ключ на host для user чтобы включить логин без пароля и по ключам

wget -r www.example.com загружает рекурсивно содержимое сайта

wget -с [www.example.com/file.iso](http://www.example.com/file.iso) загружает рекурсивно содержимое сайта

journalctl просмотр логи сервиса sshd (фикс-ся все события в системе, в том числе неудачные попытки входы по ssh).

**Wi-FI**

sudo apt-get install aircrack-ng — устанавливаем пакет

*1 Перевод сетевого адаптера в режим мониторинга*

Airmon-ng — это баш скрипт для перевода беспроводных карт в режим наблюдения. [http:aircrack-ng.org/](http://aircrack-ng.org/)

Также может использоваться для перевода из режима наблюдения в режим управляемости.

Синопсис: airmon-ng <start| stop| check> <интерфейс> [канал/частота]

Ввод команды airmon-ng без параметров отобразит статус интерфейсов.

**Start <интерфейс> [канал]** Включает режим наблюдения на интерфейсе и задает канал

**Stop <интерфейс> [канал]** Включает режим наблюдения на интерфейсе и задает канал

**check [kill]** Список программ, которые могут вмешиваться в беспроводную карту. Если указать kill, то будет сделана попытка убить их всех.

## **Примеры запуска Airmon-ng**

Просматриваем доступные сетевые интерфейсы:

sudo airmon-ng

PHY Interface   Driver      Chipset

phy0    wlan0       iwlwifi     Intel Corporation Centrino Advanced-N 6235 (rev 24)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11 | sudo airmon-ng check  Found 5 processes that could cause trouble.  If airodump-ng, aireplay-ng or airtun-ng stops working after  a short period of time, you may want to kill (some of) them!      PID Name    799 NetworkManager    894 wpa\_supplicant    905 dhclient   1089 avahi-daemon   1090 avahi-daemon |

Перед переводом в режим наблюдения, убиваем процессы, которые нам могут помешать:

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | sudo airmon-ng check kill  Killing these processes:      PID Name    894 wpa\_supplicant    905 dhclient |

Пытаемся перевести интерфейс wlan0 в режим наблюдения:

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | sudo airmon-ng start wlan0    PHY Interface   Driver      Chipset    phy0    wlan0       iwlwifi     Intel Corporation Centrino Advanced-N 6235 (rev 24)          (mac80211 monitor mode vif enabled **for** [phy0]wlan0 on [phy0]wlan0mon)          (mac80211 station mode vif disabled **for** [phy0]wlan0) |

Проверяем, была ли беспроводная карта переведена в режим монитора:

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8 | sudo iwconfig  eth0      no wireless extensions.    wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm            Retry short limit:7   RTS thr:off   Fragment thr:off            Power Management:off    lo        no wireless extensions. |

Сетевая карта изменила название интерфейса и переведена в режим монитора, наблюдения (об этом свидетельствует строка Monitor).

## **Возврат в режим управляемости**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | sudo airmon-ng stop wlan0mon    PHY Interface   Driver      Chipset    phy0    wlan0mon    rt2800usb   Ralink Technology, Corp. RT3572            (mac80211 station mode vif enabled on [phy0]wlan0)            (mac80211 monitor mode vif disabled **for** [phy0]wlan0mon) |

## **Альтернативный способ перевода в режим монитора**

Вы можете использовать альтернативный вариант перевода беспроводного интерфейса в режим наблюдения:

|  |  |
| --- | --- |
| 1  2  3 | sudo ifconfig wlan0 down  sudo iwconfig wlan0 mode monitor  sudo ifconfig wlan0 up |

***или***

|  |  |
| --- | --- |
| 1 | sudo ifconfig wlan0 down && sudo iwconfig wlan0 mode monitor && sudo ifconfig wlan0 up |

Проверяем

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8 | sudo iwconfig  eth0      no wireless extensions.    wlan0mon  IEEE 802.11abgn  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=15 dBm            Retry short limit:7   RTS thr:off   Fragment thr:off            Power Management:off    lo        no wireless extensions. |

Всё прошло успешно — сетевая карта переведена в режим наблюдения (об этом говорит строка Mode:Monitor).

Возврат в управляемый режим:

|  |  |
| --- | --- |
| 1  2  3 | ifconfig wlan0 down  iwconfig wlan0 mode managed  ifconfig wlan0 up |

## Перевод в режим монитора с помощью команд ip и iw

Команды ifconfig и iwconfig признаны устаревшими. Поэтому хотя предыдущий способ попрежнему прекрасно работает, доступна альтернативная его реализация с помощью новых программ. Узнайте имя беспроводного интерфейса:

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8 | sudo iw dev  phy#0      Interface wlan0          ifindex 5          wdev 0x3          addr 5a:88:f2:f6:52:41          type managed          txpower 20.00 dBm |

Далее выполните последовательность команд

|  |  |
| --- | --- |
| 1  2  3 | sudo ip link set <ИНТЕРФЕЙС> down  sudo iw <ИНТЕРФЕЙС> set monitor control  sudo ip link set <ИНТЕРФЕЙС> up |

|  |  |
| --- | --- |
| 1  2  3 | sudo ip link set wlan0 down  sudo iw wlan0 set monitor control  sudo ip link set wlan0 up |

Следующая большая команда должна сама определять имя беспроводного интерфейса и переводить его в режим монитора:

1 t=`sudo iw dev | grep 'Interface' | sed 's/Interface //'`;sudo ip link set $t down && sudo iw $t set monitor control && sudo ip link set $t up

Возврат в управляемый режим:

|  |  |
| --- | --- |
| 1  2  3 | sudo ip link set <ИНТЕРФЕЙС> down  sudo iw <ИНТЕРФЕЙС> set type managed  sudo ip link set <ИНТЕРФЕЙС> up |

Для интерфейса wlan0 реальные команды выглядят так:

|  |  |
| --- | --- |
| 1  2  3 | sudo ip link set wlan0 down  sudo iw wlan0 set type managed  sudo ip link set wlan0 up |

### NetworkManager препятствует переводу беспроводной карты в режим наблюдения

При определённых условиях NetworkManager может не дасть Wi-Fi адаптеру перевестись в режим монитора. Более того, уже переведённую в режим монитора беспроводную карту он может вернуть в управляемый режим. Поэтому рекомендуется отключать NetworkManager при тестировании на проникновение беспроводных сетей.

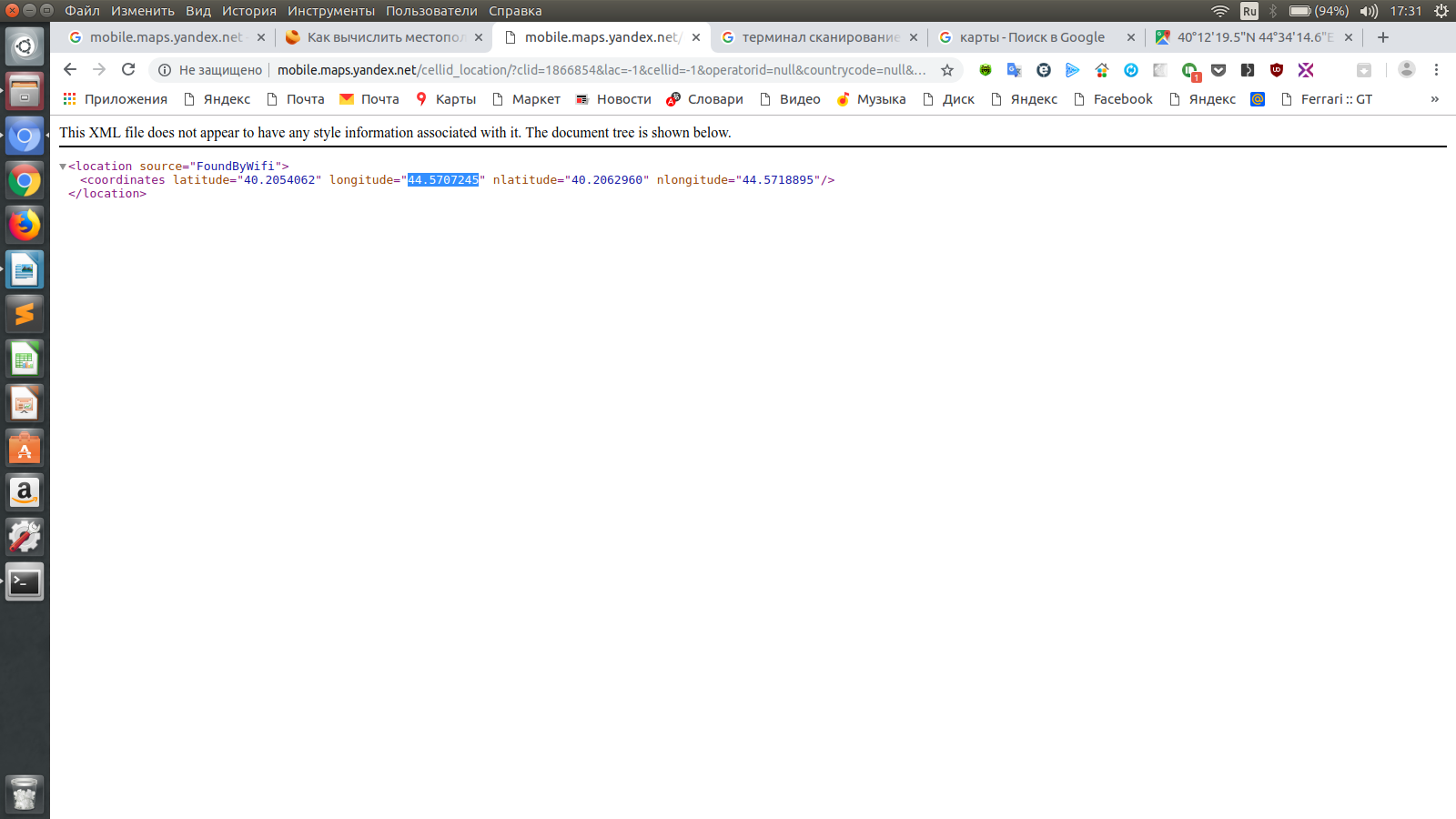
В Kali Linux и BlackArch это делается так:

|  |  |
| --- | --- |
| 1 | sudo systemctl stop NetworkManager |

Баг для определяния местоположения

<http://mobile.maps.yandex.net/cellid_location/?clid=1866854&lac=-1&cellid=-1&operatorid=null&countrycode=null&signalstrength=-1&wifinetworks=BSSID:-65&app=ymetro>

вместо BSSID вбиваем mac адрес и получим координаты для гугл карты (первые два значения)вбиваем через пробел.



Примечание, после отключения NetworkManager пропадёт Интернет

*2 Перехват пакетов*  
Airodump-ng — данная утилита используется для перехвата пакетов в беспроводной сети. Обязательно указывается название беспроводного адаптера. Перед использованием убедитесь, что включен режим монитора.

Если не указывается канал, на котором ведётся перехват, то утилита будет заставлять адаптер перескакивать с одного канала на другой. При этом этот режим даст нам информацию сходную с той, что даёт Kismet

airodump-ng wifi0

Следует учесть то, что такой режим пойдёт только для разведки. Для сбора пакетов необходимо “слушать” на конкретном канале (например на 5-ом)

airodump-ng —channel 5 wifi0

***Kali Linux***

**01- information Gathering (Сбор информаии)**

dmitry

dnmap-clie…

dnmap-ser…

like-scan

maltegoce

netdiscover

nmap

p0f

recon-ng

sparta

zenmap

**02- Vulnerabity Analysis (Анализ уязвимости)**

golismero

lynis

nikto

nmap

sparta

unix-prives

**03-Web Application Analysis (Анализ веб приложений)**

burpsuite

commix

httrack

owasp-zap

paros

skipfish

sqlmap

webscarab

wpscan

MySQL

DROP DATABASE name; //удалить БД с именем name

SHOW DATABASES; // показать Базы данных

CREATE DATABASE name; // создать БД с именем name

USE name; // перейти к БД

// создание таблицы и заполняем поля

CREATE TABLE nametable ( // создаем таблицу с именем name

- id INT AUTO\_INCREMENT PRIMARY KEY, // первое поле, целочисленное значение, авто инктемент

- name VARCHAR (30), // поле name тип символьный (30 символов)

- age INT ); //поле age численное

DESC nametable; // просмотр структуры таблицы

SHOW TABLES;// показать таблицы БД

// вносим данные в таблицу

INSERT INTO nametable VALUES (NULL, „Ivan“, 26);

// выбираем данные из таблицы

SELECT\*FROM nametable; // выбирает все данные из таблицы

SELECT id, age FROM nametable; // выбирает поля для запроса

SELECT id, age FROM nametable WHERE id=1; // выбирает поля для запроса где id=1

UPDATE nametable SET name =“NEW“, age = 13 WHERE id=2; // заменить значение на NEW и возраст на 13 где id=2

//удаляем данные из таблицы

**DELETE** FROM nametable WHERE id=2;

***Поля таблицы***

// Добавление полей таблицы

ALTER TABLE autos

- **ADD COLUMN** probeg INT AFTER nombere; // добавляем поле probeg после поля nomber

UPDATE autos SET probeg1 = 10000 WHERE id=1; // добавление данных в поля

// Удаляем поля из таблицы

ALTER TABLE autos

- **DROP COLUMN** probeg; // удаляем поле probeg из autos

// Изменить название поля

ALTER TABLE autos

**- CHANGE COLUMN** probeg1 probeg VARCHAR (15); // меняем название поля с probeg1 на probeg

// Добовляем внешний ключ

ALTER TABLE table1

- ADD FOREIGN KEY (id\_name) REFERENCES table2 (id);

***Псевдоними***

SELECT a.model, a.owner FROM autos a;

SELECT a.model new\_model, a.owner hozain FROM autos a;

***Объединяет значения полей «CONCAT»***

SELECT CONCAT (model, nomber) FROM autos;// выводит объединив

SELECT CONCAT (model, **SPACE (3)**,nomber) FROM autos; // ставит пробел между значениями

пример:

UPDATE autos SET fullname = CONCAT (model, SPACE (1), zavod); // объединяет в одном поле значения двух полей

***ASCII***

SELECT **ASCII** (model) FROM autos WHERE id=2; // выводит код первого символа

SELECT **LEFT** (model, 3) FROM autos; // выводит 3 левых символа

SELECT **RIGHT** (model, 4) FROM autos; // вывоит 4 правых символа

SELECT **LOWER** (model) FROM autos; // выводит все символы строчными

SELECT **UPPER** (model) FROM autos; // выводит все символы заглавными

SELECT **LTRIM** (model) FROM autos// выводит убрав пробелы слева

SELECT **RTRIM** (model) FROM autos// выводит убрав пробелы справа

SELECT **REPLACE** (model, „dai“, „xxx“) FROM autos; // выводит заменив dai на xxx

SELECT **REVERSE** (model) FROM autos; // выводит символы в обратной последовательности

***Указываем диапазон значений «BETWEEN»***

SELECT \*FROM users WHERE age **BETWEEN** 10 **AND** 20; // выводит значения в диапазоне от 10 до 20 вкл-но

**Выборка значений «LIKE» //** имена начинающиеся на O

SELECT user\_name FROM user WHERE user\_name **LIKE** „0%“; // % означает после О могут быть любые символы

**Объединение запросов в один «UNION»**

SELECT id FROM users **UNION** SELECT user\_name FROM users;

***Группировка данных «GROUP» (COUNT, SUM, AVG)***

SELECT user\_name, **AVG** (age) FROM users **GROUP BY** user\_mame; // выводит средний возраст у двух одинаковых user\_name

AVG -среднее значение;

MIN - минимальное значение;

MAX - максимальное значение,;

SUM - сумма значений;

COUNT — количество значений.

***Фильтрование повторяющихся данных***

SELECT DISTINCT user\_name FROM user;//выводит без повторений

***Сортировка в алфавитном порядке или по возрастанию***

SELECT\*FROM users ORDER BY user\_name; // сортируется поле user\_name

SELECT\*FROM user ORDER BY id DESC; // сортировка в порядке убывания

***DESC -***обратный порядок; ***ASC —*** прямой порядок;

***Лимит вывода данных:***

SELECT\*FROM users LIMIT 5; // выведит 5 первых записей

SELECT\*FROM users ORDER BY id DESC LIMIT 5;// выведит 5 последних записей

***Запрос из разных таблиц***

SELECT bookshop.NAME, bookshop.FAMILY, Books.title FROM bookshop, Books WHERE bookshop.bookID=Books.bookID;

***Запрос внутри запроса***

SELECT \*

FROM Orders

WHERE snum = (

SELECT snum

FROM Salespeople

WHERE sname = 'Сидоров'

) может вывести только одно значение в подзапросе.

SELECT \*

FROM Orders

WHERE snum IN (

SELECT snum

FROM Salespeople

WHERE sname = 'Сидоров'

) может вывести только несколько значений в подзапросе подзапросе.

Кодировка в UTF-8 mysql (ubuntu)

SHOW VARIABLES LIKE „char%“; - вывод значений кодировки

JDBC Connectivity in Ubuntu

sudo apt-get install mysql-server

mysql -u root -p

create database testdb;

create user «testuser»@ «localhost» identified by «password»;

grand all on testdb.\* to «testuser»;

or

create database testdb;

grand all on testdb.\*to «testuser» identified by «password»;

exit

mysql -u testuser -p

use testdb;

create table customers (customer\_id INT NOT NULL AUTO\_INCREMENT PRIMARY KEY, first\_name TEXT, last\_name