

## 1) Настройка фильтрации пакетов (фаервол)

Сначала смотрим список правил iptables по умолчанию.

```
ararata@kali:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

С более подробными значениями.

```
ararata@kali:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination
```

Посмотрим данный список в другом формате, который отражает команды, необходимые для активации правил и политик.

```
ararata@kali:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
```

Нам надо заблокировать весь исходящий трафик, кроме портов для SSH и веб-сервера, но для этого нужно сначала разрешить подключения к этим портам. В цепочку ACCEPT добавим два порта (порт SSH 22 и порт http 80), чтобы разрешить трафик на эти порты.

```
ararata@kali:~$ sudo iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
ararata@kali:~$ sudo iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
ararata@kali:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ararata@kali:~$
```

В лабораторной работе по пентесту нам не нужен был SSH, поэтому удалим его.

```

ararat@kali:~$ sudo iptables -D INPUT -p tcp -m tcp --dport 22 -j ACCEPT
ararat@kali:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     tcp  --  anywhere               anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ararat@kali:~$

```

Добавим правило, которое позволит устанавливать исходящие соединения (т.е. использовать ping или запускать обновления программного обеспечения).

```

ararat@kali:~$ sudo iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
ararat@kali:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  anywhere               anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere               anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ararat@kali:~$

```

Создав все эти правила, можно заблокировать все остальное и разрешить все исходящие соединения.

```

ararat@kali:~$ sudo iptables -P OUTPUT ACCEPT
ararat@kali:~$ sudo iptables -P INPUT DROP
ararat@kali:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere               anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere               anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ararat@kali:~$

```

Добавим еще несколько правил для блокировки наиболее распространенных атак.



```

ararat@kali:~$ sudo iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
ararat@kali:~$ sudo iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
ararat@kali:~$ sudo iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
ararat@kali:~$ iptables -L
bash: iptables: команда не найдена
ararat@kali:~$ sudo iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
ACCEPT tcp -- anywhere anywhere tcp dpt:http
DROP tcp -- anywhere anywhere tcp flags:FIN,SYN,RST,PSH,ACK,URG/NONE
DROP tcp -- anywhere anywhere tcp flags:!FIN,SYN,RST,ACK/SYN state NEW
DROP tcp -- anywhere anywhere tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN,SYN,RST,PSH,
ACK,URG

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
ararat@kali:~$

```

## 2) Мониторинг журналов с использованием logcheck

Сначала надо установить *logcheck*.

```

ararat@kali:~$ sudo apt-get install logcheck
[sudo] пароль для ararat:
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  exim4-base exim4-config exim4-daemon-light guile-2.2-libs libgnutls-dane0 libgsasl7 libipc-signal-perl
  libkyotocabinet16v5 liblockfile1 libmailutils6 libmime-types-perl libntlm0 libproc-waitstat-perl libunbound8
  lockfile-progs logcheck logcheck-database logtail mailutils mailutils-common mime-construct
Предлагаемые пакеты:
  exim4-doc-html | exim4-doc-info eximon4 spf-tools-perl libmojolicious-perl syslog-summary mailutils-mh
  mailutils-doc
Следующие НОВЫЕ пакеты будут установлены:
  exim4-base exim4-config exim4-daemon-light guile-2.2-libs libgnutls-dane0 libgsasl7 libipc-signal-perl
  libkyotocabinet16v5 liblockfile1 libmailutils6 libmime-types-perl libntlm0 libproc-waitstat-perl libunbound8
  lockfile-progs logcheck logcheck-database logtail mailutils mailutils-common mime-construct
Обновлено 0 пакетов, установлено 21 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.
Необходимо скачать 10,9 МВ архивов.
После данной операции объём занятого дискового пространства возрастёт на 59,5 МБ.
Хотите продолжить? [Д/н] y
Пол:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 exim4-config all 4.93-16 [328 kB]
Пол:2 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 exim4-base amd64 4.93-16 [1153 kB]
Пол:3 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 libunbound8 amd64 1.10.0-1 [485 kB]
Пол:4 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 libgnutls-dane0 amd64 3.6.13-2 [361 kB]
Пол:5 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 exim4-daemon-light amd64 4.93-16 [627 kB]
Пол:6 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 guile-2.2-libs amd64 2.2.7+1-5 [4979 kB]
Пол:7 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 libntlm0 amd64 1.6-1+b1 [23,5 kB]

```

*Logcheck* успешно установлен.

```

Настраивается пакет libproc-waitstat-perl (1.00-5) ...
Настраивается пакет lockfile-progs (0.1.18) ...
Настраивается пакет exim4-daemon-light (4.93-16) ...
Настраивается пакет libmailutils6:amd64 (1:3.7-2.1) ...
Настраивается пакет mailutils (1:3.7-2.1) ...
update-alternatives: используется /usr/bin/frm.mailutils для предоставления /usr/bin/frm (frm) в автоматическом ре
жиме
update-alternatives: используется /usr/bin/from.mailutils для предоставления /usr/bin/from (from) в автоматическом
режиме
update-alternatives: используется /usr/bin/messages.mailutils для предоставления /usr/bin/messages (messages) в ав
томатическом режиме
update-alternatives: используется /usr/bin/movemail.mailutils для предоставления /usr/bin/movemail (movemail) в ав
томатическом режиме
update-alternatives: используется /usr/bin/readmsg.mailutils для предоставления /usr/bin/readmsg (readmsg) в автом
атическом режиме
update-alternatives: используется /usr/bin/dotlock.mailutils для предоставления /usr/bin/dotlock (dotlock) в автом
атическом режиме
update-alternatives: используется /usr/bin/mail.mailutils для предоставления /usr/bin/mailx (mailx) в автоматическ
ом режиме
Настраивается пакет mime-construct (1.11+nmv2) ...
Настраивается пакет logcheck (1.3.20) ...
Добавление пользователя logcheck в группу adm
Обрабатываются триггеры для libc-bin (2.30-4) ...
Обрабатываются триггеры для systemd (245.5-2) ...
Обрабатываются триггеры для man-db (2.9.1-1) ...
Обрабатываются триггеры для kali-menu (2020.2.2) ...
ararat@kali:~$

```

Открываем в редакторе *nano* файл *logcheck.conf*

```
ararat@kali: ~  
Файл Действия Правка Вид Справка  
GNU nano 4.9.2 /etc/logcheck/logcheck.conf  
# The following variable settings are the initial default values,  
# which can be uncommented and modified to alter logcheck's behaviour  
  
# Controls the format of date-/time-stamps in subject lines:  
# Alternatively, set the format to suit your locale  
#DATE="$(date +%Y-%m-%d %H:%M%)"  
  
# Controls the presence of boilerplate at the top of each message:  
# Alternatively, set to "0" to disable the introduction.  
#  
# If the files /etc/logcheck/header.txt and /etc/logcheck/footer.txt  
# are present their contents will be read and used as the header and  
# footer of any generated mails.  
  
#INTRO=1  
  
# Controls the level of filtering:  
# Can be Set to "workstation", "server" or "paranoid" for different  
# levels of filtering. Defaults to server if not set.  
  
REPORTLEVEL="server"
```

Меняем параметр REPORTLEVEL с «server» на «paranoid»



```
ararat@kali: ~  
Файл Действия Правка Вид Справка  
GNU nano 4.9.2 /etc/logcheck/logcheck.conf  
# Controls the presence of boilerplate at the top of each message:  
# Alternatively, set to "0" to disable the introduction.  
#  
# If the files /etc/logcheck/header.txt and /etc/logcheck/footer.txt  
# are present their contents will be read and used as the header and  
# footer of any generated mails.  
  
#INTRO=1  
  
# Controls the level of filtering:  
# Can be Set to "workstation", "server" or "paranoid" for different  
# levels of filtering. Defaults to server if not set.  
  
REPORTLEVEL="paranoid"  
  
# Controls the address mail goes to:  
# *NOTE* the script does not set a default value for this variable!  
# Should be set to an offsite "emailaddress@some.domain.tld"  
  
SENDMAILTO="logcheck"  
  
# Send the results as attachment or not.  
# 0=not as attachment; 1=as attachment; 2=as gzip attachment
```

Смотрим логи

```
ararat@kali: ~  
Файл Действия Правка Вид Справка  
May 13 19:44:34 kali systemd[1]: Reloading.  
May 13 19:44:34 kali systemd[1]: /lib/systemd/system/dbus.socket:5: ListenStream= references a path below legacy d  
irectory /var/run/, updating /var/run/dbus/system_bus_socket → /run/dbus/system_bus_socket; please update the unit  
file accordingly.  
May 13 19:44:40 kali dbus-daemon[474]: [system] Activating via systemd: service name='org.freedesktop.PackageKit'  
unit='packagekit.service' requested by ':1.65' (uid=0 pid=2631 comm="/usr/bin/gdbus call --system --dest org.freed  
esktopto")  
May 13 19:44:40 kali systemd[1]: Starting PackageKit Daemon ...  
May 13 19:44:40 kali PackageKit: daemon start  
May 13 19:44:40 kali dbus-daemon[474]: [system] Successfully activated service 'org.freedesktop.PackageKit'  
May 13 19:44:40 kali systemd[1]: Started PackageKit Daemon.  
May 13 19:46:46 kali dbus-daemon[803]: [session uid=1000 pid=803] Activating service name='org.freedesktop.thumbna  
ils.Thumbnailer1' requested by ':1.69' (uid=1000 pid=1136 comm="Thunar --sm-client-id 23c692cf3-541b-4a97-b47c-59d  
")  
May 13 19:46:47 kali org.freedesktop.thumbnails.Thumbnailer1[2657]: Registered thumbnailer /usr/bin/gdk-pixbuf-thu  
mbnailer -s %s %u %o  
May 13 19:46:47 kali org.freedesktop.thumbnails.Thumbnailer1[2657]: Registered thumbnailer /usr/bin/gdk-pixbuf-thu  
mbnailer -s %s %u %o  
May 13 19:46:47 kali org.freedesktop.thumbnails.Thumbnailer1[2657]: Registered thumbnailer atril-thumbnailer -s %s  
%u %o  
May 13 19:46:47 kali dbus-daemon[803]: [session uid=1000 pid=803] Successfully activated service 'org.freedesktop.  
thumbnails.Thumbnailer1'  
May 13 19:49:46 kali PackageKit: daemon quit  
May 13 19:49:46 kali systemd[1]: packagekit.service: Succeeded.  
  
ararat@kali:~$  
ararat@kali:~$
```

### 3) Установка и настройка netfilter

**В этом пункте необходимо продемонстрировать возможности именно netfilter. Сделаем это на примере conntrack. Используем модуль отслеживания состояния пакетов conntrack.**

В первом пункте данной работы мы писали правила фильтрации с TCP-флагами, в этот раз мы воспользуемся модулем conntrack, который помечает каждый пакет специальными метками.

```
ararat@kali:~$ sudo iptables -A INPUT -i eth0 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
ararat@kali:~$ sudo iptables -A INPUT -i eth0 -p tcp --dport 80 -m conntrack --ctstate NEW -j ACCEPT
ararat@kali:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere              tcp dpt:http ctstate NEW
ACCEPT     tcp  --  anywhere              anywhere             

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ararat@kali:~$
```

Мы реализовали глобальное разрешение только входящих ESTABLISHED, RELATED пакетов на любые порты внешнего интерфейса. Входящие ESTABLISHED, RELATED пакеты могут появиться только после инициирования TCP-соединений извне по конкретному порту, который мы и прописали отдельно (порт 80).

Далее, для полного контроля над ситуацией, можем сопоставлять метки, назначенные пакету модулем conntrack с актуальным состоянием битов в них с помощью опции `--tcp-flags` для параметра `-p tcp`.

```
ararat@kali:~$ sudo iptables -A INPUT -m conntrack --ctstate NEW,INVALID -p tcp --tcp-flags SYN,ACK SYN,ACK -j REJECT --reject-with tcp-reset
ararat@kali:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere              tcp dpt:http ctstate NEW
REJECT     tcp  --  anywhere              anywhere              ctstate INVALID,NEW tcp flags:SYN,ACK/SYN,ACK reject
--with tcp-reset

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

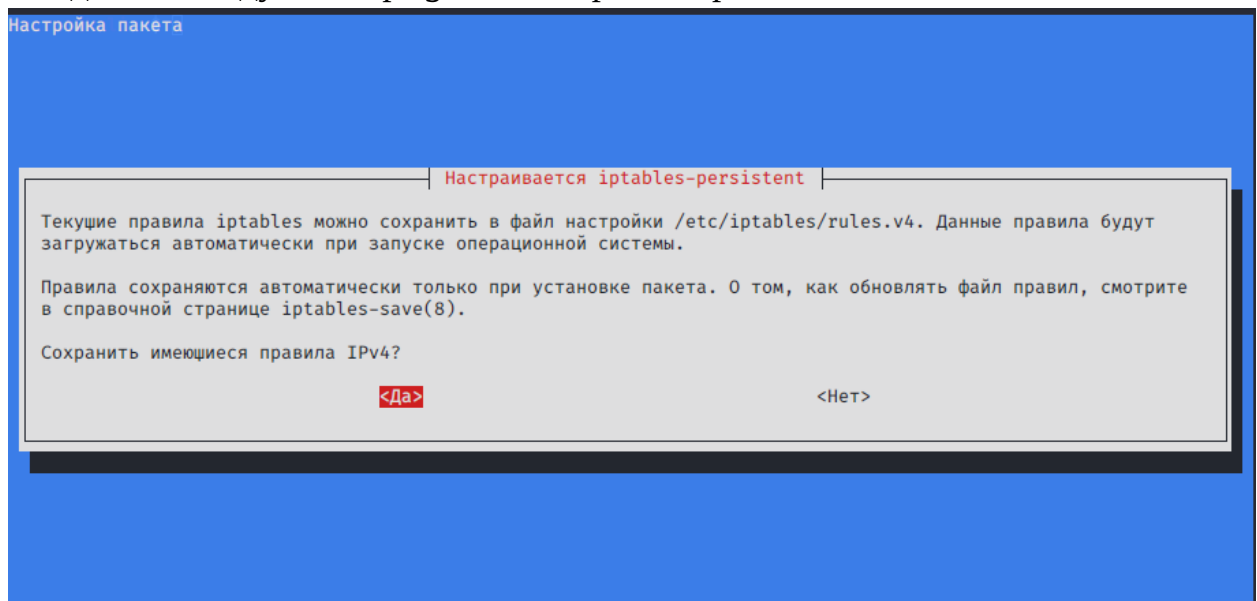
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ararat@kali:~$
```

#### **4) Осуществить защиту файловой системы.**

Реализуем защиту файловой системы с помощью iptables. Также сделаем так, чтобы правила сохранились после перезагрузки.

```
ararat@kali: ~  
  
Файл Действия Правка Вид Справка  
ararat@kali:~$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE  
ararat@kali:~$ sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT  
ararat@kali:~$ cat /proc/sys/net/ipv4/ip_forward  
0  
ararat@kali:~$ sudo bash -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'  
ararat@kali:~$ cat /proc/sys/net/ipv4/ip_forward  
1  
ararat@kali:~$ █
```

Вводим команду *sudo apt-get install iptables-persistent*.



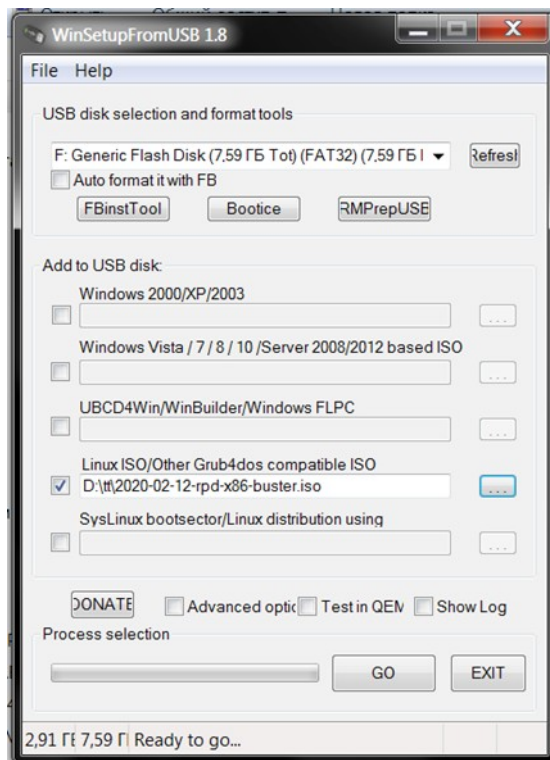
Пакет *iptables-persistent* успешно установлен.

```
iptables-persistent netfilter-persistent  
Обновлено 0 пакетов, установлено 2 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.  
Необходимо скачать 22,9 кВ архивов.  
После данной операции объём занятого дискового пространства возрастёт на 87,0 кВ.  
Хотите продолжить? [Д/н] у  
Пол:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 netfilter-persistent all 1.0.14 [10,6 kB]  
Пол:2 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 iptables-persistent all 1.0.14 [12,3 kB]  
Получено 22,9 кВ за 2с (9903 В/с)  
Предварительная настройка пакетов ...  
Выбор ранее не выбранного пакета netfilter-persistent.  
(Чтение базы данных ... на данный момент установлено 292192 файла и каталога.)  
Подготовка к распаковке ./netfilter-persistent_1.0.14_all.deb ...  
Распаковывается netfilter-persistent (1.0.14) ...  
Выбор ранее не выбранного пакета iptables-persistent.  
Подготовка к распаковке ./iptables-persistent_1.0.14_all.deb ...  
Распаковывается iptables-persistent (1.0.14) ...  
Настраивается пакет netfilter-persistent (1.0.14) ...  
update-rc.d: We have no instructions for the netfilter-persistent init script.  
update-rc.d: It looks like a non-network service, we enable it.  
netfilter-persistent.service is a disabled or a static unit, not starting it.  
Настраивается пакет iptables-persistent (1.0.14) ...  
update-alternatives: используется /lib/systemd/system/netfilter-persistent.service для предоставления /lib/systemd  
/system/iptables.service (iptables.service) в автоматическом режиме  
Обрабатываются триггеры для systemd (245.5-2) ...  
Обрабатываются триггеры для man-db (2.9.1-1) ...  
Обрабатываются триггеры для kali-menu (2020.2.2) ...  
ararat@kali:~$ █
```

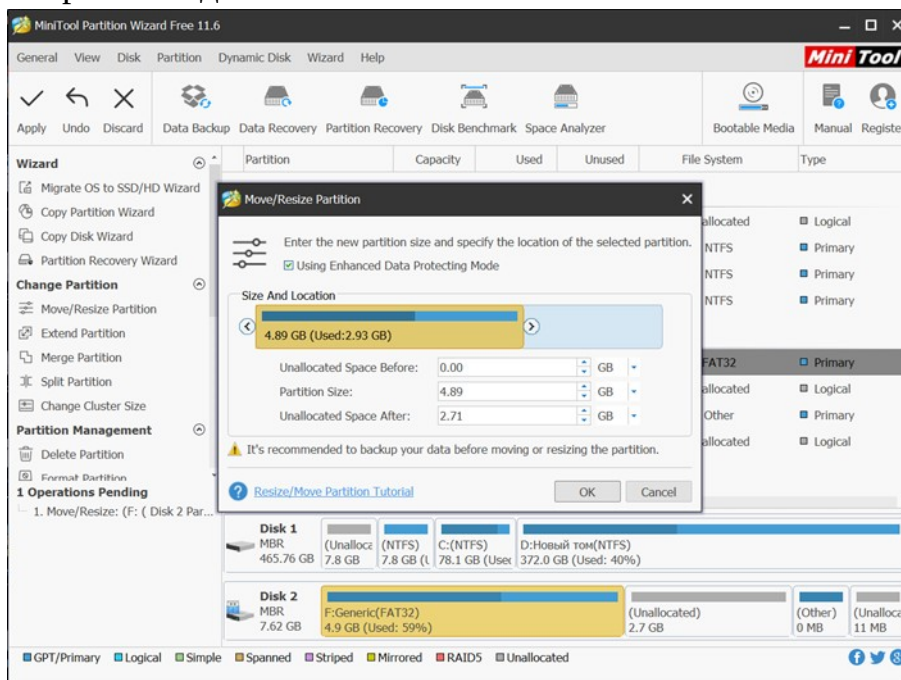
## 5) Установка Kali Linux с флешки

Сделаем из обычной флешки загрузочную.



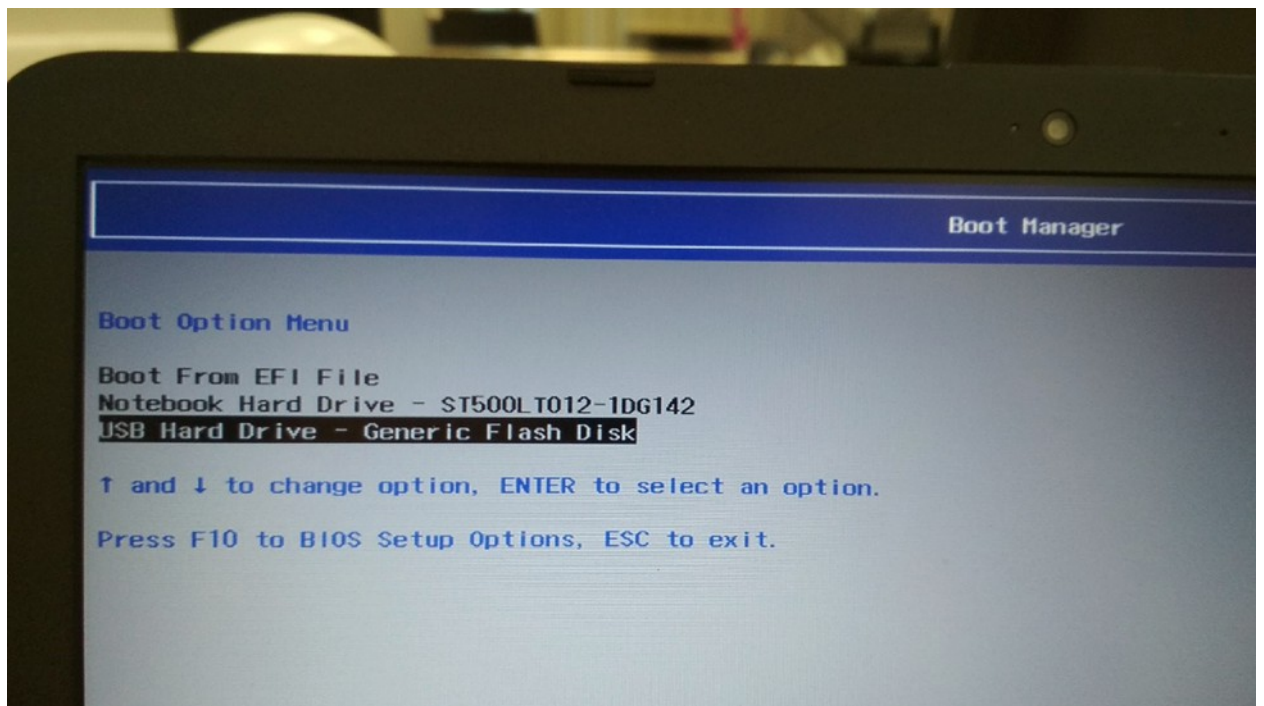


Далее на загрузочной флешке зарезервируем свободное место для сохранения данных.

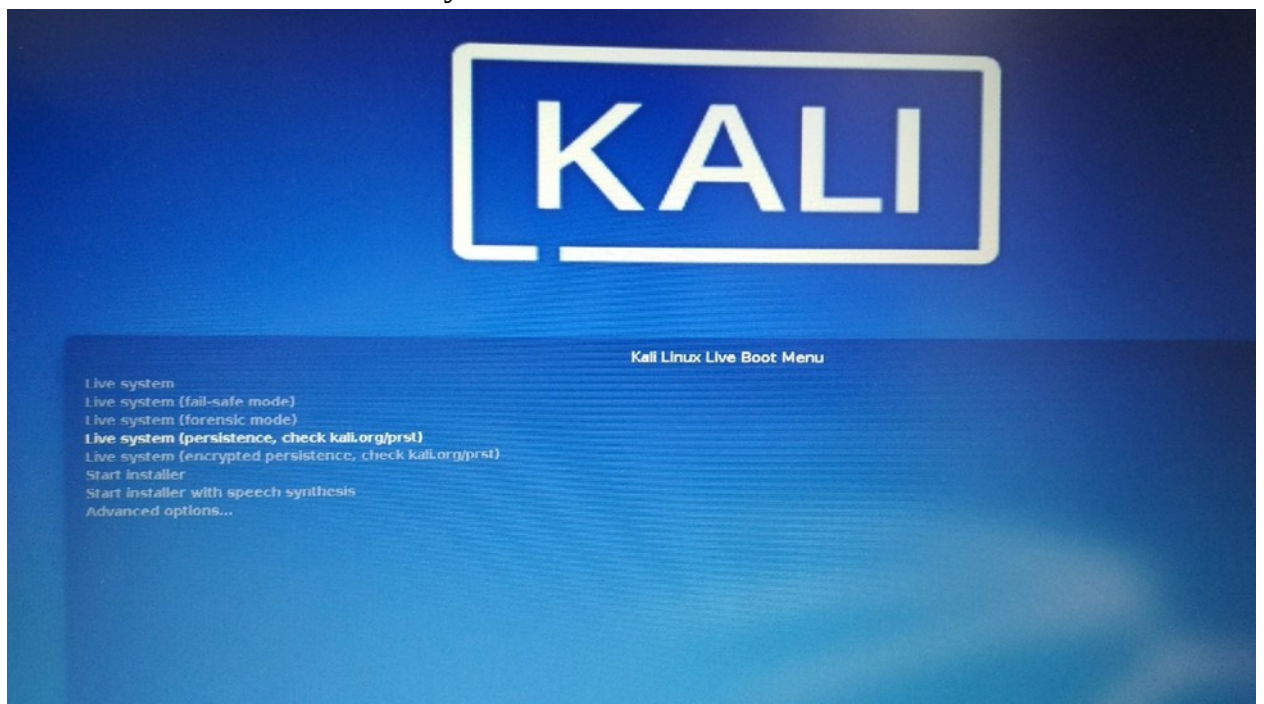


Затем перезагружаем компьютер и заходим в Boot Menu. Там выбираем, нашу флешку и запускаемся с неё.





После этого в окне Kali запускаем её.



## 6) Установка LOIC на Kali Linux.

Сначала установим пакет git-core через утилиту dpkg.

```
ararat@kali: ~  
Файл Действия Правка Вид Справка  
ararat@kali:~$ wget http://ftp.br.debian.org/debian/pool/main/g/git/git-core_2.1.4-2.1+deb8u6_all.deb  
--2020-05-18 01:00:00-- http://ftp.br.debian.org/debian/pool/main/g/git/git-core_2.1.4-2.1+deb8u6_all.deb  
Распознаётся ftp.br.debian.org (ftp.br.debian.org)... 200.236.31.3, 2801:82:80ff:8000::4  
Подключение к ftp.br.debian.org (ftp.br.debian.org)|200.236.31.3|:80 ... соединение установлено.  
HTTP-запрос отправлен. Ожидание ответа... 200 OK  
Длина: 1506 (1,5K) [application/x-debian-package]  
Сохранение в: «git-core_2.1.4-2.1+deb8u6_all.deb»  
  
git-core_2.1.4-2.1 100%[=====] 1,47K --KB/s за 0s  
  
2020-05-18 01:00:01 (117 MB/s) - «git-core_2.1.4-2.1+deb8u6_all.deb» сохранён [1506/1506]  
ararat@kali:~$ sudo dpkg -i git-core_2.1.4-2.1+deb8u6_all.deb  
[sudo] пароль для ararat:  
Выбор ранее не выбранного пакета git-core.  
(Чтение базы данных ... на данный момент установлено 322729 файлов и каталогов.)  
Подготовка к распаковке git-core_2.1.4-2.1+deb8u6_all.deb ...  
Распаковывается git-core (1:2.1.4-2.1+deb8u6) ...  
Настраивается пакет git-core (1:2.1.4-2.1+deb8u6) ...  
ararat@kali:~$
```

Проверим, что git-core установлен.

```
ararat@kali:~$ sudo apt list --installed | grep git-core  
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.  
git-core/now 1:2.1.4-2.1+deb8u6 all [установлен, локальный]  
ararat@kali:~$ sudo apt list --installed | grep git-core  
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.  
git-core/now 1:2.1.4-2.1+deb8u6 all [установлен, локальный]  
ararat@kali:~$
```

Далее надо установить пакет *monodevelop*. Для этого переходим на официальный сайт <https://www.monodevelop.com/>, находим там инструкцию для установки *monodevelop* на Linux.



## Debian 8 (i386, amd64, armhf, armel)

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 3FA7E0328081BFF6A14DA29AA6A19B38D3D831EF
sudo apt install apt-transport-https
echo "deb https://download.mono-project.com/repo/debian vs-jessie main" | sudo tee /etc/apt/sources.list.d/mono-official-vs.list
sudo apt update
```

## ② Install MonoDevelop

```
sudo apt-get install monodevelop
```

The package **monodevelop** should be installed for the MonoDevelop IDE.

Далее, точно следуя всем инструкциям устанавливаем MonoDevelop на Kali Linux.

```
ararat@kali: ~  
Файл Действия Правка Вид Справка  
ararat@kali:~$ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 3FA7E0328081BFF6A14DA29AA6A19B38D3D831EF  
Executing: /tmp/apt-key-gpghome.3SWaK76Ymt/gpg.1.sh --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 3FA7E0328081BFF6A14DA29AA6A19B38D3D831EF  
gpg: ключ A6A19B38D3D831EF: импортирован открытый ключ "Xamarin Public Jenkins (auto-signing) <releng@xamarin.com>"  
gpg: Всего обработано: 1  
gpg: импортировано: 1  
ararat@kali:~$  
ararat@kali:~$ sudo apt install apt-transport-https  
Чтение списков пакетов... Готово  
Построение дерева зависимостей  
Чтение информации о состоянии... Готово  
Следующие НОВЫЕ пакеты будут установлены:  
  apt-transport-https  
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.  
Необходимо скачать 154 kB архивов.  
После данной операции объем занятого дискового пространства возрастёт на 161 kB.  
Пол:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 apt-transport-https all 2.1.2 [154 kB]  
Получено 154 kB за 1с (142 kB/s)  
Выбор ранее не выбранного пакета apt-transport-https.  
(Чтение базы данных ... на данный момент установлено 328784 файла и каталога.)  
Подготовка к распаковке .../apt-transport-https_2.1.2_all.deb ...  
Распаковывается apt-transport-https (2.1.2) ...  
Настраивается пакет apt-transport-https (2.1.2) ...  
ararat@kali:~$
```

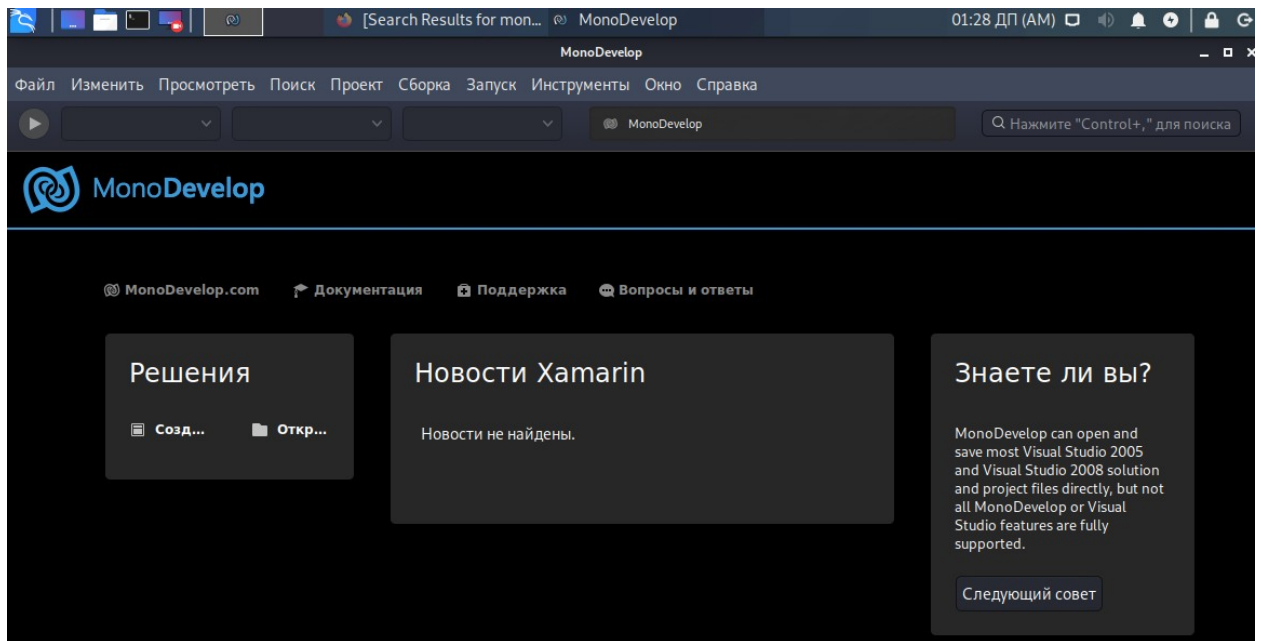
```
ararat@kali:~$ echo "deb https://download.mono-project.com/repo/debian vs-jessie main" | sudo tee /etc/apt/sources.list.d/mono-official-vs.list  
deb https://download.mono-project.com/repo/debian vs-jessie main  
ararat@kali:~$
```



```
ararat@kali:~$ sudo apt update
Пол:1 https://download.mono-project.com/repo/debian vs-jessie InRelease [5874 B]
Суш:2 http://mirror-1.truenetwork.ru/kali kali-rolling InRelease
Пол:3 https://download.mono-project.com/repo/debian vs-jessie/main amd64 Packages [49,2 kB]
Получено 55,1 kB за 1с (37,3 kB/s)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Все пакеты имеют последние версии.
ararat@kali:~$
```

```
ararat@kali:~$ sudo apt-get install monodevelop
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
ca-certificates-mono cli-common fsharp gnome-icon-theme
libfsharp-core4.3-cil libgdiplus libglade2-0 libglade2.0-cil
libglib2.0-cil libglib2.0-cil-dev libgtk2.0-cil libgtk2.0-cil-dev
libmono-2.0-dev libmono-accessibility4.0-cil
libmono-btls-interface4.0-cil libmono-cairo4.0-cil
libmono-cecil-private-cil libmono-cil-dev libmono-codecontracts4.0-cil
libmono-compilerservices-symbolwriter4.0-cil libmono-corlib4.5-cil
libmono-cscompgd0.0-cil libmono-csharp4.0c-cil
libmono-custommarshalers4.0-cil libmono-data-tds4.0-cil
libmono-db2-1.0-cil libmono-debugger-soft4.0a-cil libmono-http4.0-cil
libmono-i18n-cjk4.0-cil libmono-i18n-mideast4.0-cil
libmono-i18n-other4.0-cil libmono-i18n-rare4.0-cil
libmono-i18n-west4.0-cil libmono-i18n4.0-all libmono-i18n4.0-cil
libmono-ldap4.0-cil libmono-management4.0-cil
libmono-messaging-rabbitmq4.0-cil libmono-messaging4.0-cil
libmono-microsoft-build-engine4.0-cil
libmono-microsoft-build-framework4.0-cil
libmono-microsoft-build-tasks-v4.0-4.0-cil
libmono-microsoft-build-utilities-v4.0-4.0-cil
libmono-microsoft-build4.0-cil libmono-microsoft-csharp4.0-cil
libmono-microsoft-visualc10.0-cil
ararat@kali:~$
```

Чтобы убедиться в том, что MonoDevelop успешно установился, откроем его и посмотрим на интерфейс.



Теперь мы готовы к установке собственно самого LOIC. Для этого создадим на рабочем столе папку под названием "loic" и скачаем туда файл *loic.sh*.

```
ararat@kali:~/Рабочий стол$ mkdir loic
ararat@kali:~/Рабочий стол$ cd loic
ararat@kali:~/Рабочий стол/loic$ ls -l
итого 0
ararat@kali:~/Рабочий стол/loic$ wget https://www.dropbox.com/s/m2gqm8b4v5c5ib/loic.sh
--2020-05-18 16:10:50-- https://www.dropbox.com/s/m2gqm8b4v5c5ib/loic.sh
Распознаётся www.dropbox.com (www.dropbox.com)... 162.125.70.1, 2620:100:6026:1::a27d:4601
Подключение к www.dropbox.com (www.dropbox.com)|162.125.70.1|:443... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 301 Moved Permanently
Адрес: /s/raw/m2gqm8b4v5c5ib/loic.sh [переход]
--2020-05-18 16:10:51-- https://www.dropbox.com/s/raw/m2gqm8b4v5c5ib/loic.sh
Повторное использование соединения с www.dropbox.com:443.
HTTP-запрос отправлен. Ожидание ответа... 302 Found
Адрес: https://uca984ae21af2275cbfe3a3bfb4.dl.dropboxusercontent.com/cd/0/inline/A3_BKcqSlos5bYSJtQeqLcbtQYJxEsqHEXJyEmv84_MX1s0-2ERlc2wxTkPY-eUB84qAPR8wRKLLpubnkyQITcqUHNf656pZ8320qB9Sw71NEA/file# [переход]
--2020-05-18 16:10:51-- https://uca984ae21af2275cbfe3a3bfb4.dl.dropboxusercontent.com/cd/0/inline/A3_BKcqSlos5bYSJtQeqLcbtQYJxEsqHEXJyEmv84_MX1s0-2ERlc2wxTkPY-eUB84qAPR8wRKLLpubnkyQITcqUHNf656pZ8320qB9Sw71NEA/file
Распознаётся uca984ae21af2275cbfe3a3bfb4.dl.dropboxusercontent.com (uca984ae21af2275cbfe3a3bfb4.dl.dropboxusercontent.com)... 162.125.70.6, 2620:100:6026:6::a27d:4606
Подключение к uca984ae21af2275cbfe3a3bfb4.dl.dropboxusercontent.com (uca984ae21af2275cbfe3a3bfb4.dl.dropboxusercontent.com)|162.125.70.6|:443... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 200 OK
Длина: 2331 (2,3К) [text/plain]
Сохранение в: «loic.sh»
```

Настроим права на выполнение.

```
ararat@kali:~/Рабочий стол/loic$ ls -l
итого 4
-rw-r--r-- 1 ararat ararat 2331 мая 18 16:10 loic.sh
ararat@kali:~/Рабочий стол/loic$ sudo chmod a+x loic.sh
[sudo] пароль для ararat:
ararat@kali:~/Рабочий стол/loic$ ls -l
итого 4
-rwxr-xr-x 1 ararat ararat 2331 мая 18 16:10 loic.sh
ararat@kali:~/Рабочий стол/loic$
```

Далее, нам надо отредактировать файл *loic.sh*. В методе *compile\_loic()* меняем строку "*mdtool build*" на "*cd src; xbuild*".



До отредактирования:

```
compile_loic() {  
    get_loic  
    if ! is_loic ; then  
        echo "Error: You are not in a LOIC repository."  
        exit 1  
    fi  
    if [[ $DISTRO = 'ubuntu' || $DISTRO = 'debian' ]] ; then  
        sudo apt-get install $DEB_MONO_PKGS  
    elif [[ $DISTRO = 'fedora' ]] ; then  
        sudo yum install $FED_MONO_PKGS  
    fi  
    mdtool build  
}
```

После отредактирования:

```
compile_loic() {  
    get_loic  
    if ! is_loic ; then  
        echo "Error: You are not in a LOIC repository."  
        exit 1  
    fi  
    if [[ $DISTRO = 'ubuntu' || $DISTRO = 'debian' ]] ; then  
        sudo apt-get install $DEB_MONO_PKGS  
    elif [[ $DISTRO = 'fedora' ]] ; then  
        sudo yum install $FED_MONO_PKGS  
    fi  
    cd src; xbuild  
}
```

Далее, переход в папку *loic* и устанавливаем одноимённую программу.

```
ararat@kali: ~/Рабочий стол/loic  
Файл Действия Правка Вид Справка  
ararat@kali:~/Рабочий стол$ cd loic  
ararat@kali:~/Рабочий стол/loic$ ./loic.sh install  
/usr/bin/git  
Клонирование в «LOIC»...  
warning: переадресация на https://github.com/NewEraCracker/LOIC.git/  
remote: Enumerating objects: 1915, done.  
remote: Total 1915 (delta 0), reused 0 (delta 0), pack-reused 1915  
Получение объектов: 100% (1915/1915), 4.28 MiB | 2.24 MiB/s, готово.  
Определение изменений: 100% (1191/1191), готово.  
  
>>>> xbuild tool is deprecated and will be removed in future updates, use msbuild instead <<<  
<  
  
XBuild Engine Version 14.0  
Mono, Version 6.8.0.105  
Copyright (C) 2005-2013 Various Mono authors  
  
Build started 18.05.2020 16:19:31.  
  
Project "/home/ararat/Рабочий стол/loic/LOIC/src/LOIC.sln" (default target(s)):  
  Target ValidateSolutionConfiguration:  
    Building solution configuration "Debug|Any CPU".  
  Target Build:  
    Project "/home/ararat/Рабочий стол/loic/LOIC/src/IRC/IRC.csproj" (default target(s)):  
    Target PrepareForBuild:  
      Configuration: Debug Platform: AnyCPU
```



```
ararat@kali:~/Рабочий стол/loic$ ./loic.sh update
/usr/bin/git
warning: переадресация на https://github.com/NewEraCracker/LOIC.git/
Уже обновлено.
Current branch master is up to date.
/usr/bin/git

>>>> xbuild tool is deprecated and will be removed in future updates, use msbuild instead <<<
<

XBuild Engine Version 14.0
Mono, Version 6.8.0.105
Copyright (C) 2005-2013 Various Mono authors

Build started 18.05.2020 16:20:14.

-----
Project "/home/ararat/Рабочий стол/loic/LOIC/src/LOIC.sln" (default target(s)):
  Target ValidateSolutionConfiguration:
    Building solution configuration "Debug|Any CPU".
  Target Build:
    Project "/home/ararat/Рабочий стол/loic/LOIC/src/IRC/IRC.csproj" (default target(s)):
```

Запускаем LOIC.

```
ararat@kali:~/Рабочий стол/loic$ ./loic.sh run
/usr/bin/git

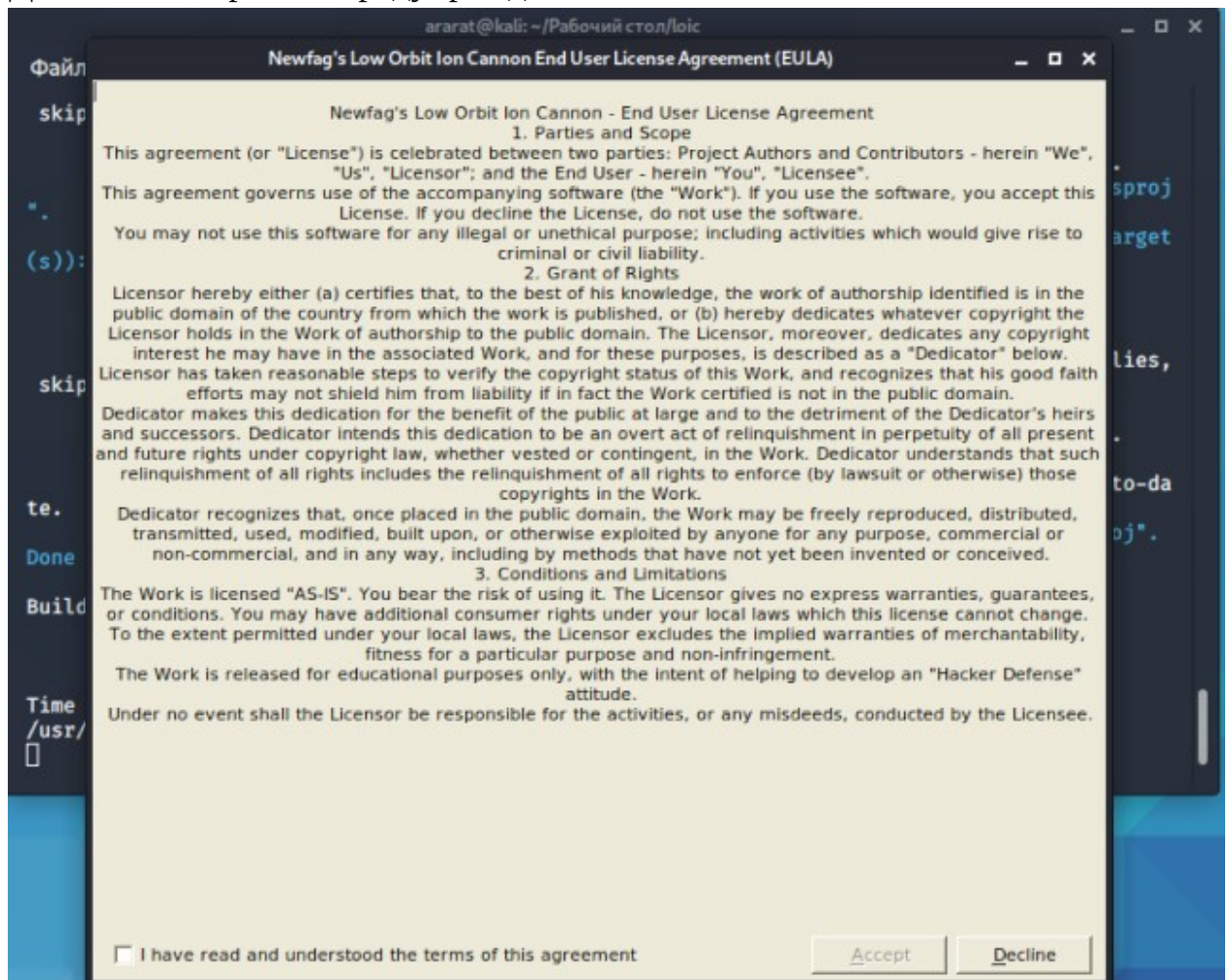
>>>> xbuild tool is deprecated and will be removed in future updates, use msbuild instead <<<
<

XBuild Engine Version 14.0
Mono, Version 6.8.0.105
Copyright (C) 2005-2013 Various Mono authors

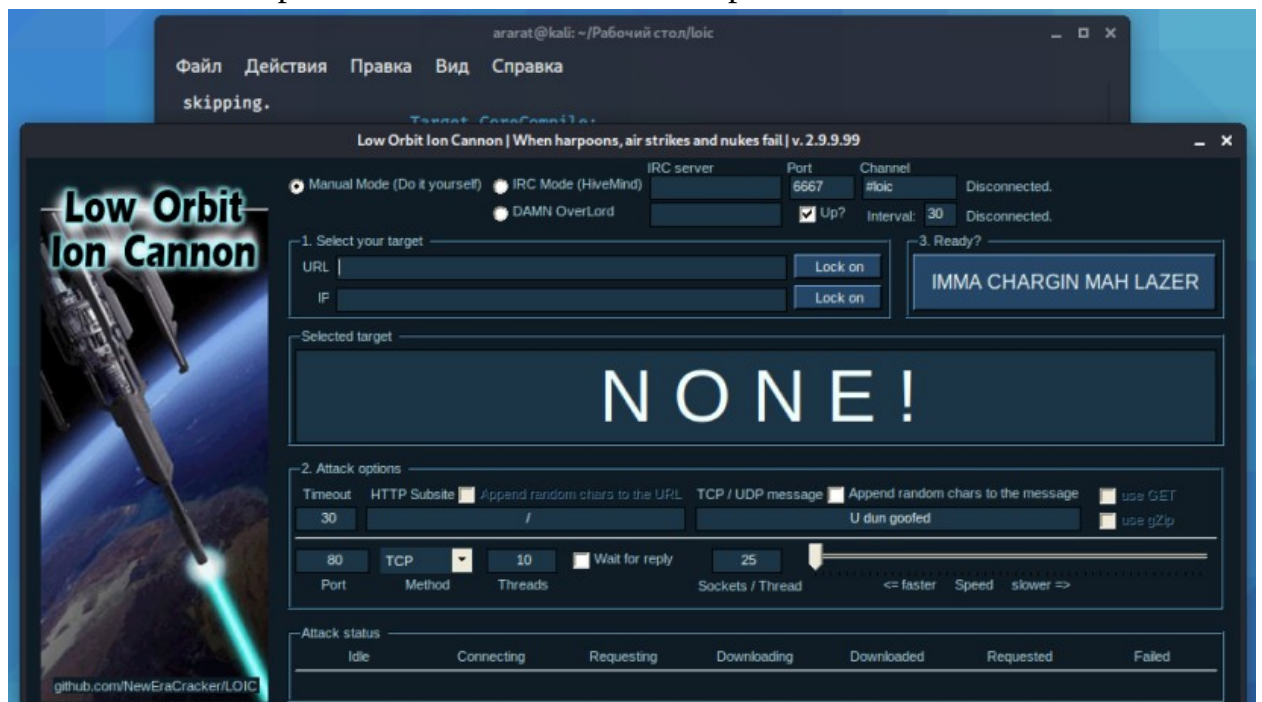
Build started 18.05.2020 16:20:57.

-----
Project "/home/ararat/Рабочий стол/loic/LOIC/src/LOIC.sln" (default target(s)):
  Target ValidateSolutionConfiguration:
    Building solution configuration "Debug|Any CPU".
  Target Build:
    Project "/home/ararat/Рабочий стол/loic/LOIC/src/IRC/IRC.csproj" (default target(s)):
      Target PrepareForBuild:
        Configuration: Debug Platform: AnyCPU
      Target GenerateSatelliteAssemblies:
        No input files were specified for target GenerateSatelliteAssemblies,
        skipping.
      Target CoreCompile:
        Skipping target "CoreCompile" because its outputs are up-to-date.
```

Далее, нас встречает предупреждение.



Соглашаемся с правилами - нажимаем «Ассерпт»



## 7) Установка Wifi\_Jammer на Kali Linux.

Скачаем с github репозиторий *wifijammer* и перейдём в папку.

```
ararat@kali: ~/wifijammer
Файл Действия Правка Вид Справка
ararat@kali:~$ git clone https://github.com/DanMcInerney/wifijammer.git
Клонирование в «wifijammer»...
remote: Enumerating objects: 274, done.
remote: Total 274 (delta 0), reused 0 (delta 0), pack-reused 274
Получение объектов: 100% (274/274), 82.17 KiB | 472.00 KiB/s, готово.
Определение изменений: 100% (111/111), готово.
ararat@kali:~$ cd wifijammer/
ararat@kali:~/wifijammer$
```

Попытаемся запустить программу.

```
ararat@kali:~$ cd wifijammer/
ararat@kali:~/wifijammer$ sudo python2 wifijammer.py --help
[sudo] пароль для ararat:
python2: can't open file 'wifijammer.py': [Errno 2] No such file or directory
ararat@kali:~/wifijammer$ sudo python2 wifijammer --help
Traceback (most recent call last):
  File "wifijammer", line 6, in <module>
    from scapy.all import *
ImportError: No module named scapy.all
```

Если внимательно прочитать ошибку, то можно понять, что необходимо установить пакет *python-scapy*.

```
ararat@kali:~/wifijammer$ sudo apt-get install python-scapy
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Предлагаемые пакеты:
  python-matplotlib python-pyx sox
Рекомендуемые пакеты:
  ipython python-cryptography
Следующие НОВЫЕ пакеты будут установлены:
  python-scapy
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновле-
но.
Необходимо скачать 695 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 4 471 kB.
Пол:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 python-scapy all 2.4.3-3 [695 kB]
Получено 695 kB за 1с (505 kB/s)
Выбор ранее не выбранного пакета python-scapy.
(Чтение базы данных ... на данный момент установлено 335437 файлов и каталогов.)
Подготовка к распаковке ./python-scapy_2.4.3-3_all.deb ...
Распаковывается python-scapy (2.4.3-3) ...
Настраивается пакет python-scapy (2.4.3-3) ...
Обрабатываются триггеры для man-db (2.9.1-1) ...
Обрабатываются триггеры для kali-menu (2020.2.2) ...
ararat@kali:~/wifijammer$
```



```


ararat@kali: ~/wifijammer
Файл Действия Правка Вид Справка

ararat@kali:~/wifijammer$ sudo python2 wifijammer --help
usage: wifijammer [-h] [-s [SKIP [SKIP ... ]]] [-i INTERFACE] [-c CHANNEL]
                  [-m MAXIMUM] [-n] [-t TIMEINTERVAL] [-p PACKETS] [-d]
                  [-a [ACCESSPOINT [ACCESSPOINT ... ]]] [--world] [--dry-run]

optional arguments:
  -h, --help                show this help message and exit
  -s [SKIP [SKIP ... ]], --skip [SKIP [SKIP ... ]]
                            Skip deauthing this MAC address. Example: -s
                            00:11:BB:33:44:AA
  -i INTERFACE, --interface INTERFACE
                            Choose monitor mode interface. By default script will
                            find the most powerful interface and starts monitor
                            mode on it. Example: -i mon5
  -c CHANNEL, --channel CHANNEL
                            Listen on and deauth only clients on the specified
                            channel. Example: -c 6
  -m MAXIMUM, --maximum MAXIMUM
                            Choose the maximum number of clients to deauth. List
                            of clients will be emptied and repopulated after
                            hitting the limit. Example: -m 5
  -n, --noupdate            Do not clear the deauth list when the maximum (-m)
                            number of client/AP combos is reached. Must be used in
                            conjunction with -m. Example: -m 10 -n
  -t TIMEINTERVAL, --timeinterval TIMEINTERVAL
                            Choose the time interval between packets being sent.
                            Default is as fast as possible. If you see scapy
                            errors like 'no buffer space' try: -t .00001
  -p PACKETS, --packets PACKETS
                            Choose the number of packets to send in each deauth
                            burst. Default value is 1; 1 packet to the client and
                            1 packet to the AP. Send 2 deauth packets to the
                            client and 2 deauth packets to the AP: -p 2
  -d, --directedonly        Skip the deauthentication packets to the broadcast
                            address of the access points and only send them to
                            client/AP pairs
  -a [ACCESSPOINT [ACCESSPOINT ... ]], --accesspoint [ACCESSPOINT [ACCESSPOINT ... ]]

```

## Протестируем через SQLMAP сайт кафедры ЗСС.

```
ararat@kali: ~  
Файл Действия Правка Вид Справка  
ararat@kali:~$ sudo sqlmap -u http://zss.sut.ru --batch  
 {1.4.5#stable}  
http://sqlmap.org  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting @ 21:11:43 /2020-05-18/  
[21:11:43] [INFO] testing connection to the target URL  
you have not declared cookie(s), while server wants to set its own ('language=ru'). Do you want to use those [Y/n] Y  
[21:11:47] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS  
[21:11:47] [INFO] testing if the target URL content is stable  
[21:11:49] [INFO] target URL content is stable  
[21:11:49] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2'  
[*] ending @ 21:11:49 /2020-05-18/  
ararat@kali:~$
```



Теперь попробуем сохранить в файл.

```
ararat@kali:~$ crunch 9 9 0123 -o passwords.txt
Crunch will now generate the following amount of data: 2621440 bytes
2 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 262144

crunch: 100% completed generating output
ararat@kali:~$
```

Как видим, появился файл.

```
ararat@kali:~$ ls -l
итого 8752
-rw-r--r-- 1 ararat ararat 1506 мая 29 2018 git-core_2.1.4-2.1+deb8u6_all.deb
-rw-r--r-- 1 ararat ararat 6296200 дек 15 2014 monodevelop_4.0.12+dfsg-6_all.deb
-rw-r--r-- 1 ararat ararat 2621440 мая 18 22:07 passwords.txt
drwxr-xr-x 3 ararat ararat 4096 мая 18 17:10 wifijammer
drwxr-xr-x 2 ararat ararat 4096 мая 18 00:25 Видео
drwxr-xr-x 2 ararat ararat 4096 мая 18 00:25 Документы
drwxr-xr-x 2 ararat ararat 4096 мая 18 01:44 Загрузки
drwxr-xr-x 2 ararat ararat 4096 мая 18 00:25 Изображения
drwxr-xr-x 2 ararat ararat 4096 мая 18 00:25 Музыка
drwxr-xr-x 2 ararat ararat 4096 мая 18 00:25 Общедоступные
drwxr-xr-x 3 ararat ararat 4096 мая 18 16:08 'Рабочий стол'
drwxr-xr-x 2 ararat ararat 4096 мая 18 00:25 Шаблоны
ararat@kali:~$
```

Откроем файл.

passwords.txt (-) - GVIM

Файл Правка Инструменты Синтаксис Буферы Окно Справка

112202010  
 112202011  
 112202012  
 112202013  
 112202020  
 112202021  
 112202022  
 112202023  
 112202030  
 112202031  
 112202032  
 112202033  
 112202100  
 112202101  
 112202102  
 112202103  
 112202110  
 112202111  
 112202112  
 112202113  
 112202120  
 112202121  
 112202122

92298,1 35%