Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Лабораторная работа №1

Выполнили студенты группы ИКТЗ-83:

Громов А.А., Миколаени М.С., Мазеин Д.С.

(Ф.И.О., № группы)

_____

(подпись)

Проверил:

Казанцев А.А.

_____

(*уч. степень, уч. звание, Ф.И.О.)*

(подпись)

Санкт-Петербург

2021

Часть 1 - Настройка фильтрации пакетов (фаервол)

Рис. 1 Выводим список правил iptables.

Рис. 2 Выводим список правил iptables подробнее.

Рис. 3 Выводим список команд необходимых для активации правил и политик.

Рис. 4 Разрешаем трафик на 80 и 22 порты для tcp протокола.

```
iktz-83@kali     ~     sudo iptables -D INPUT -p tcp -m tcp --dport 22 -j ACCEPT
iktz-83@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
 iktz-83@kali     ~
```

Рис. 5 Удаляем разрешение для порта 22.

```
 iktz-83@kali     ~     sudo iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
 iktz-83@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
 iktz-83@kali     ~
```
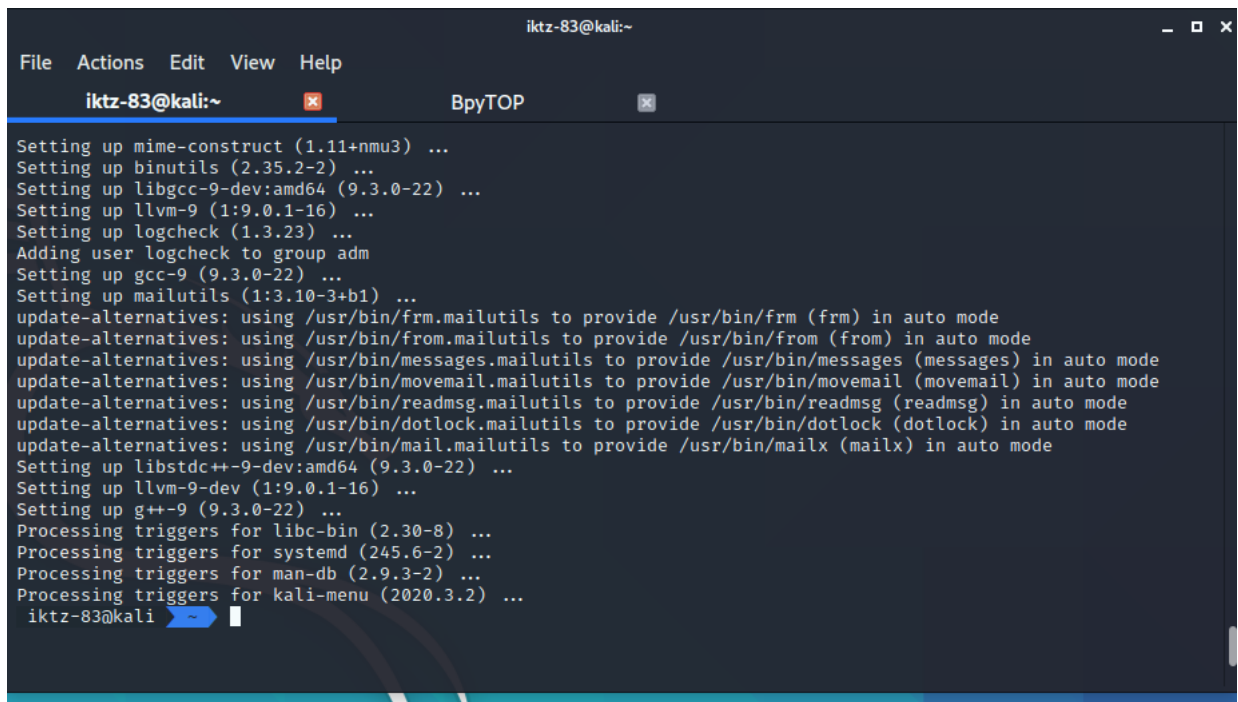
Рис. 6 Правило, позволяющее устанавливать исходящее соединение.

```
 iktz-83@kali     ~     sudo iptables -P OUTPUT ACCEPT
 iktz-83@kali     ~     sudo iptables -P INPUT DROP
 iktz-83@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
 iktz-83@kali     ~
```
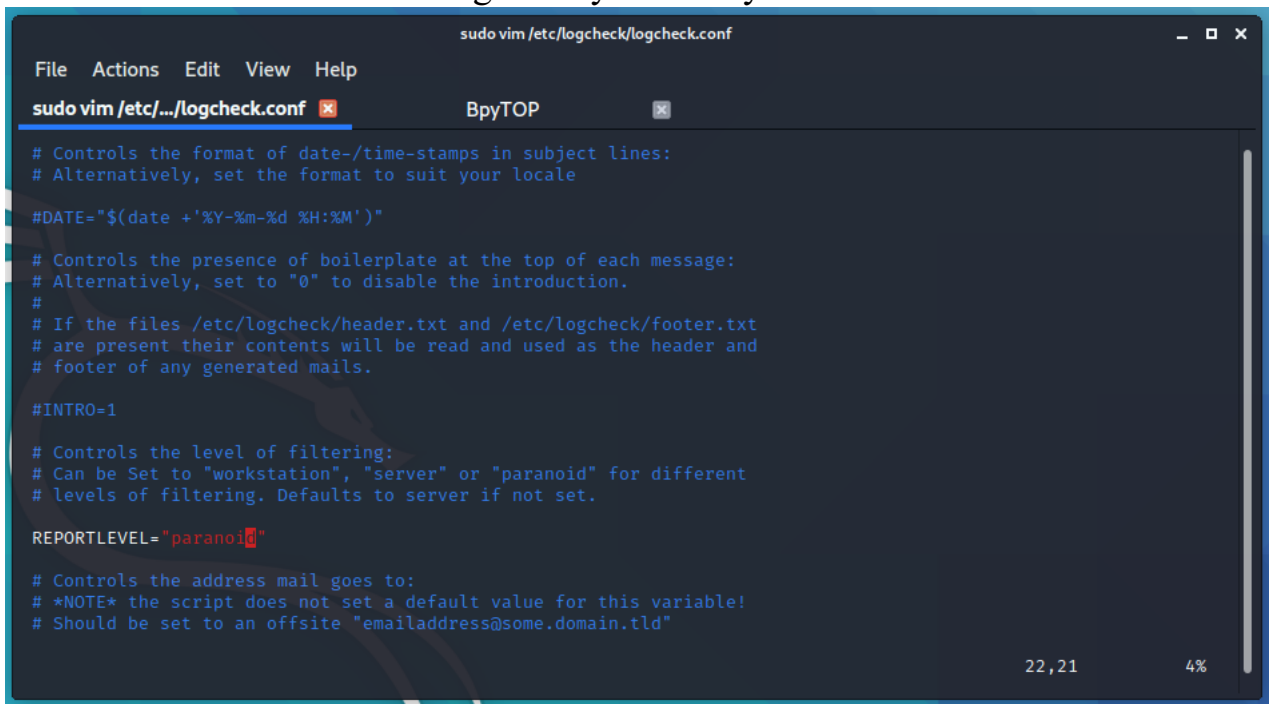
Рис. 7 Запрещаем все входящие и разрешаем все исходящие.

```
target     prot opt source              destination
 iktz-83@kali     ~     sudo iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
 iktz-83@kali     ~     sudo iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
 iktz-83@kali     ~     sudo iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
 iktz-83@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
 iktz-83@kali     ~
```

Рис. 8 Правила для блокировки наиболее распространенных атак.

Часть 2 - Мониторинг журналов с использованием logcheck

Рис. 9 logcheck успешно установлен.

Рис. 10 Изменили REPORTLEVEL с server на paranoid

Рис. 11 Логи из файла /var/log/syslog

Часть 3 - Установка и настройка netfilter

Рис. 12 Помечаем каждый пакет с помощью модуля conntrack.

Рис. 13 Сопоставляем метки с состоянием битов.

Часть 4 - Осуществить защиту файловой системы.

```
iktz-83@kali ~ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iktz-83@kali ~ sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
iktz-83@kali ~ cat /proc/sys/net/ipv4/ip_forward
0
iktz-83@kali ~ sudo bash -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'
iktz-83@kali ~ cat /proc/sys/net/ipv4/ip_forward
1
iktz-83@kali ~ []
```

Рис. 14 Подменяем внутренный ip на внешний для всех пакетов, а также разрешаем перенаправлять пакеты между внутренними интерфейсами.

```
Do you want to continue: [Y/n] y
Get:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 netfilter-persistent all 1.0.15 [11.0 kB]
Get:2 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 iptables-persistent all 1.0.15 [12.4 kB]
Fetched 23.4 kB in 1s (17.8 kB/s)
Preconfiguring packages ...
Selecting previously unselected package netfilter-persistent.
(Reading database ... 277664 files and directories currently installed.)
Preparing to unpack .../netfilter-persistent_1.0.15_all.deb ...
Unpacking netfilter-persistent (1.0.15) ...
Selecting previously unselected package iptables-persistent.
Preparing to unpack .../iptables-persistent_1.0.15_all.deb ...
Unpacking iptables-persistent (1.0.15) ...
Setting up netfilter-persistent (1.0.15) ...
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.
Setting up iptables-persistent (1.0.15) ...
update-alternatives: using /lib/systemd/system/netfilter-persistent.service to provide /lib/systemd/system/iptables.service (i
ptables.service) in auto mode
Processing triggers for systemd (245.6-2) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2020.3.2) ...
iktz-83@kali ~ []
```

Рис. 15 Устанавливаем пакет iptables-persistent.

Часть 6 - Установка LOIC на Kali Linux.

```
x iktz-83@kali ~ wget http://ftp.br.debian.org/debian/pool/main/g/git/git-core_2.1.4-2.1+deb8u6_all.deb
--2021-04-27 16:06:03--  http://ftp.br.debian.org/debian/pool/main/g/git/git-core_2.1.4-2.1+deb8u6_all.deb
Resolving ftp.br.debian.org (ftp.br.debian.org)... 200.236.31.3, 2801:82:80ff:8000::4
Connecting to ftp.br.debian.org (ftp.br.debian.org)|200.236.31.3|:80... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 1506 (1.5K) [application/vnd.debian.binary-package]
Saving to: 'git-core_2.1.4-2.1+deb8u6_all.deb'

git-core_2.1.4-2.1+deb8u6_all.d 100%[===================>]   1.47K  --.-KB/s    in 0s

2021-04-27 16:06:04 (50.3 MB/s) - 'git-core_2.1.4-2.1+deb8u6_all.deb' saved [1506/1506]
```

Рис. 16 Скачиваем git-core

```
iktz-83@kali ~ sudo dpkg -i git-core_2.1.4-2.1+deb8u6_all.deb
Selecting previously unselected package git-core.
(Reading database ... 277690 files and directories currently installed.)
Preparing to unpack git-core_2.1.4-2.1+deb8u6_all.deb ...
Unpacking git-core (1:2.1.4-2.1+deb8u6) ...
Setting up git-core (1:2.1.4-2.1+deb8u6) ...
iktz-83@kali ~ 
```

Рис. 17 Устанавливаем git-core с помощью утилиты dpkg

```
iktz-83@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 [installed,local]
iktz-83@kali ~ []
```

Рис. 18 Проверям установился ли пакет git-core

```
iktz-83@kali ~ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 3FA7E0328081BFF6A14DA29AA6A19B38D3D
831EF
Executing: /tmp/apt-key-gpghome.LopYZGDVOE/gpg.1.sh --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 3FA7E0328081BFF6A14D
A29AA6A19B38D3D831EF


gpg: key A6A19B38D3D831EF: public key "Xamarin Public Jenkins (auto-signing) <releng@xamarin.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Рис. 19 Команда для установки MonoDevelop

6

Рис. 20 Команда для установки MonoDevelop
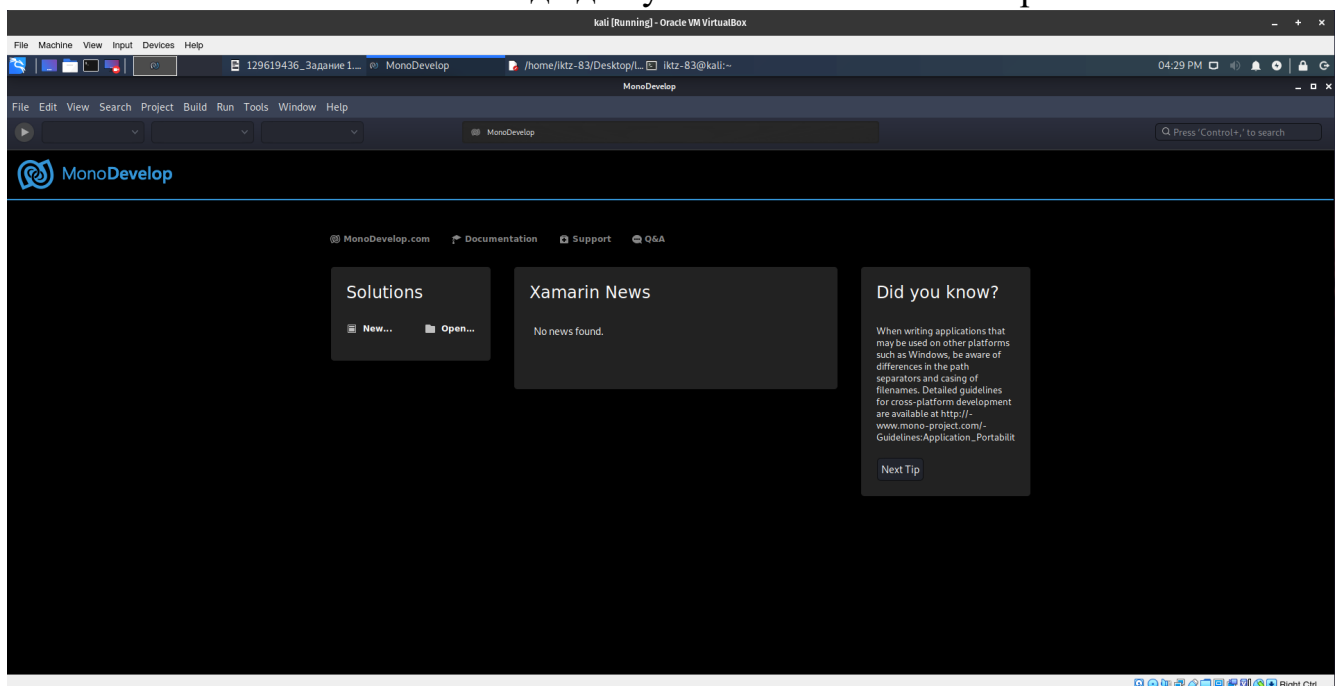

Рис. 21 Команда для установки MonoDevelop

Рис. 22 Интерфейс программы MonoDevelop

7

```
iktz-83@kali  ~  mkdir loic
iktz-83@kali  ~  cd loic
iktz-83@kali  ~/loic  ls -l
total 0
iktz-83@kali  ~/loic  wget https://www.dropbox.com/s/m2gqmq8b4v5c5ib/loic.sh
--2021-04-27 16:31:46--  https://www.dropbox.com/s/m2gqmq8b4v5c5ib/loic.sh
Resolving www.dropbox.com (www.dropbox.com)... 162.125.71.18, 2620:100:6026:18::a27d:4612
Connecting to www.dropbox.com (www.dropbox.com)|162.125.71.18|:443... connected.
HTTP request sent, awaiting response ... 301 Moved Permanently
Location: /s/raw/m2gqmq8b4v5c5ib/loic.sh [following]
--2021-04-27 16:31:47--  https://www.dropbox.com/s/raw/m2gqmq8b4v5c5ib/loic.sh
Reusing existing connection to www.dropbox.com:443.
HTTP request sent, awaiting response ... 302 Found
Location: https://uc7514cc9ee7b30317da8c2d6981.dl.dropboxusercontent.com/cd/0/inline/BNYPKCCVpAIMSDOBdmU4PDmodsSqoO6kgmITyOjTFN3Oswmkita6SJUsRB_
lVmBWiRXWbmSIcbsAeWsyZ1bjQzTZbDYpRki8dycmXcW3EGEZ6-AlWPdiJA0h_cXy3T7DL7BuVr5UxP9mPZWactP6vidm/file# [following]
--2021-04-27 16:31:48--  https://uc7514cc9ee7b30317da8c2d6981.dl.dropboxusercontent.com/cd/0/inline/BNYPKCCVpAIMSDOBdmU4PDmodsSqoO6kgmITyOjTFN3O
swmkita6SJUsRB_lVmBWiRXWbmSIcbsAeWsyZ1bjQzTZbDYpRki8dycmXcW3EGEZ6-AlWPdiJA0h_cXy3T7DL7BuVr5UxP9mPZWactP6vidm/file
Resolving uc7514cc9ee7b30317da8c2d6981.dl.dropboxusercontent.com (uc7514cc9ee7b30317da8c2d6981.dl.dropboxusercontent.com)... 162.125.71.15, 2620
:100:6026:15::a27d:460f
Connecting to uc7514cc9ee7b30317da8c2d6981.dl.dropboxusercontent.com (uc7514cc9ee7b30317da8c2d6981.dl.dropboxusercontent.com)|162.125.71.15|:443
... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 2331 (2.3K) [text/plain]
Saving to: 'loic.sh'

loic.sh                    100%[===================================>]   2.28K  --.-KB/s    in 0s

2021-04-27 16:31:48 (25.1 MB/s) - 'loic.sh' saved [2331/2331]

iktz-83@kali  ~/loic
```

Рис. 23 Создаем папку и скачиваем скрипт для установки loic

```
iktz-83@kali  ~/loic  ls -l
total 4
-rw-r--r-- 1 iktz-83 iktz-83 2331 Apr 27 16:31 loic.sh
iktz-83@kali  ~/loic  sudo chmod a+x loic.sh
[sudo] password for iktz-83:
iktz-83@kali  ~/loic  ls -l
total 4
-rwxr-xr-x 1 iktz-83 iktz-83 2331 Apr 27 16:31 loic.sh
iktz-83@kali  ~/loic
```

Рис. 24 Делаем скрипт исполняемым файлом

```
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_PKS
    fi
    cd src; xbuild
}
```

Рис. 25 Правим скрипт.

```
iktz-83@kali  ~/loic  vim loic.sh
iktz-83@kali  ~/loic  ./loic.sh install
/usr/bin/git
Cloning into 'LOIC'...
warning: redirecting to https://github.com/NewEraCracker/LOIC.git/
remote: Enumerating objects: 1915, done.
remote: Total 1915 (delta 0), reused 0 (delta 0), pack-reused 1915
Receiving objects: 100% (1915/1915), 4.28 MiB | 1.27 MiB/s, done.
Resolving deltas: 100% (1191/1191), done.

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

XBuild Engine Version 14.0
Mono, Version 6.12.0.122
Copyright (C) 2005-2013 Various Mono authors

Build started 4/28/2021 9:47:34 AM.
_____
Project "/home/iktz-83/loic/LOIC/src/LOIC.sln" (default target(s)):
        Target ValidateSolutionConfiguration:
```

Рис. 26 Запускаем установку loic.

Рис. 27 Обновляем.
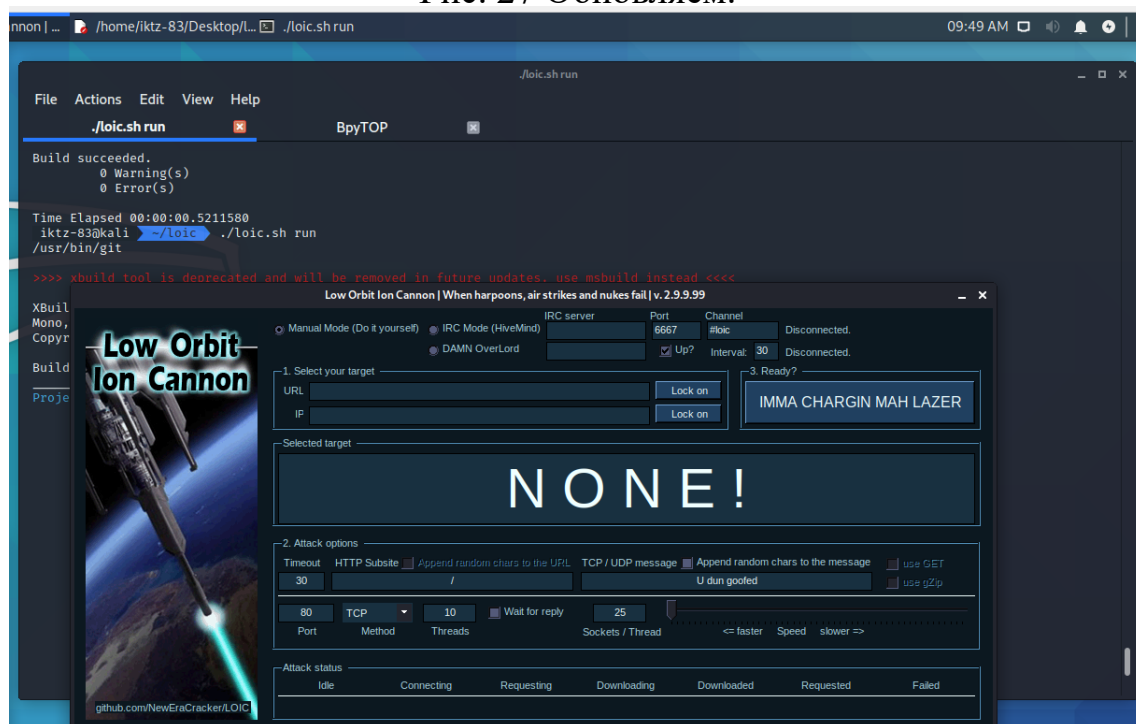
Рис. 28 Программа loic установленна, и запущена.

Часть 7 - Установка Wifi_Jammer на Kali Linux.

Рис. 29 Клонируем из репозитория на github wifijammer.git.

Рис. 30 Убеждаемся, что у нас не установовелна библиотека scapy, для python 2.

Рис. 31 wifijammer работает, после установки недостающего пакета.

Часть 8 - Использование SQLMAP на Kali Linux: взлом веб-сайтов и баз данных через SQL-инъекции

Рис. 32 Производим SQL-инъекцию со стандартным поведением.

Рис. 33 Производим SQL-инъекцию со стандартным поведением и случайным user-agent.

Часть 9 - Crunch — генератор паролей. Установка и тест.


```
  iktz-83@kali  ~  crunch 1 9 0123456789abcdefg
Crunch will now generate the following amount of data: 1252121211606 bytes
1194115 MB
1166 GB
1 TB
0 PB
Crunch will now generate the following number of lines: 125999618777
```

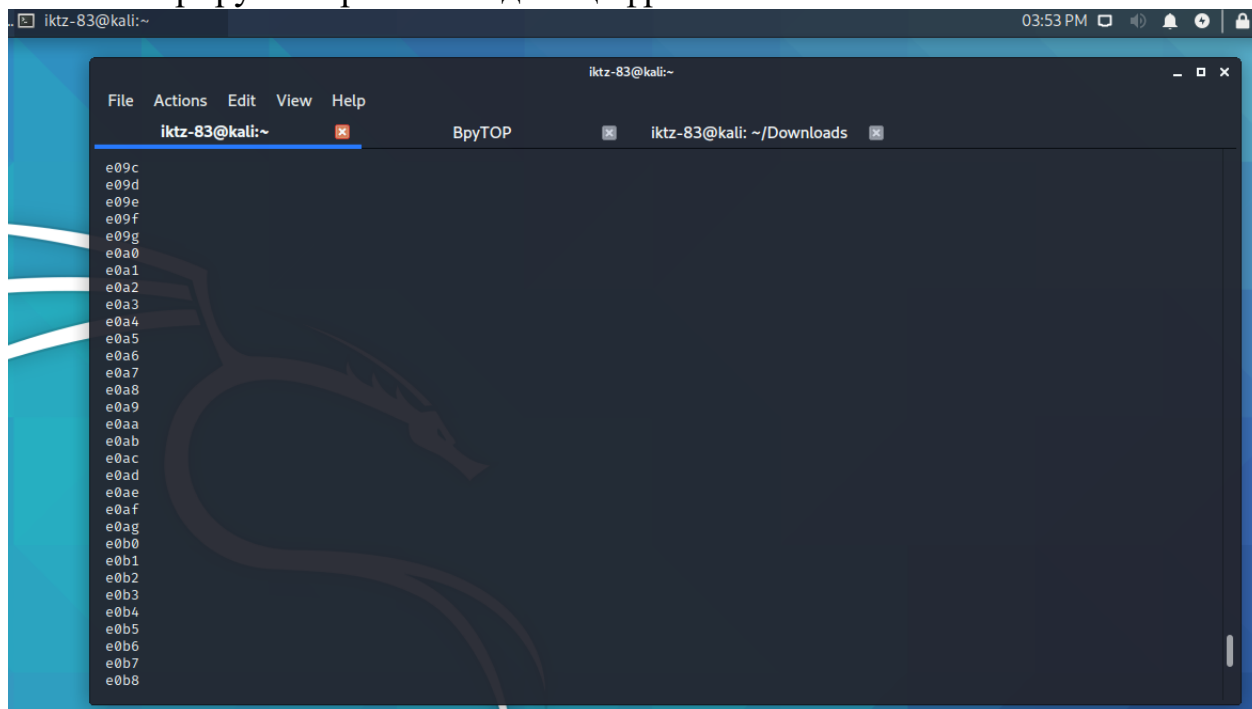Рис. 34 Генерируем пароли от 1 до 9 цифр с использованием 0123456789abcdefg.

Рис. 35 Пример паролей.


```
  x iktz-83@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
  iktz-83@kali  ~  
```

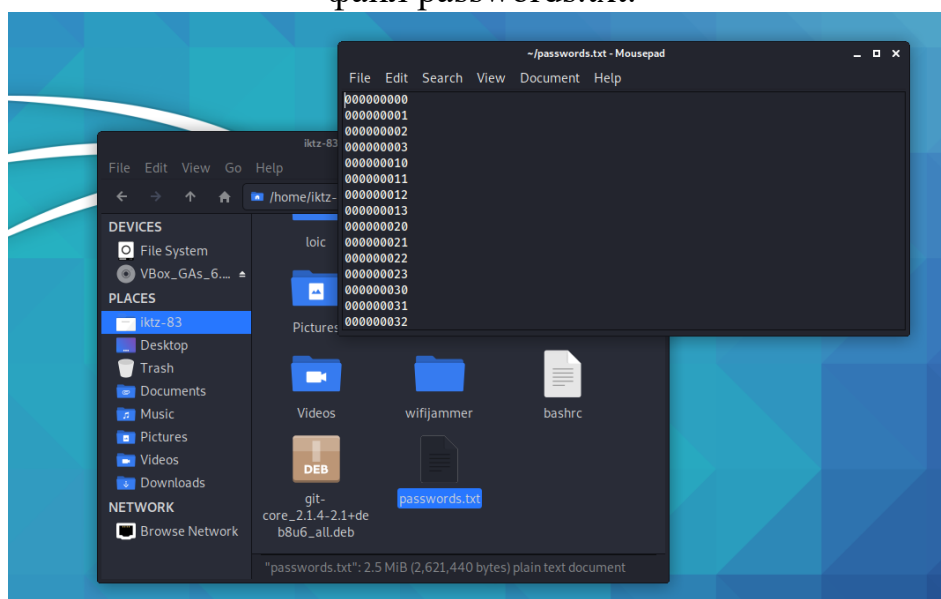Рис. 36 Генерируем пароли из 9 цифр с использованием 0123 и сохраняем их в файл passwords.txt.

Рис. 37 Проверяем файл passwords.txt.