ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

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)

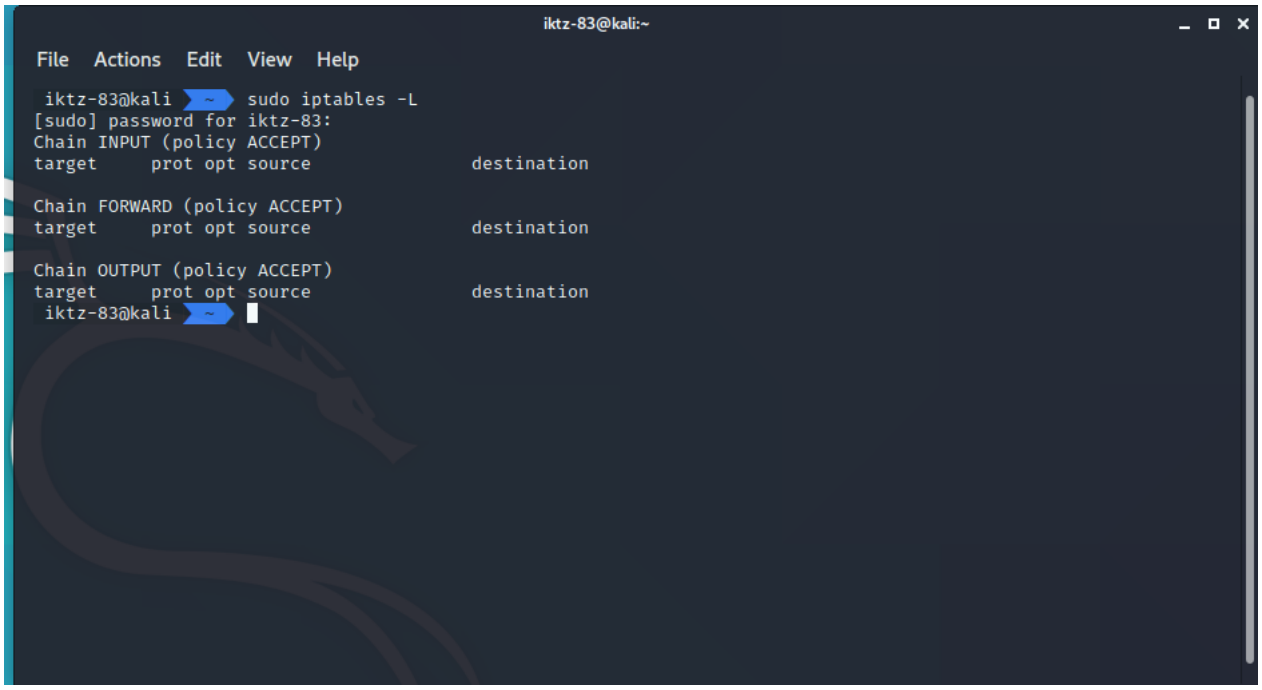

Рис. 1 Выводим список правил iptables.

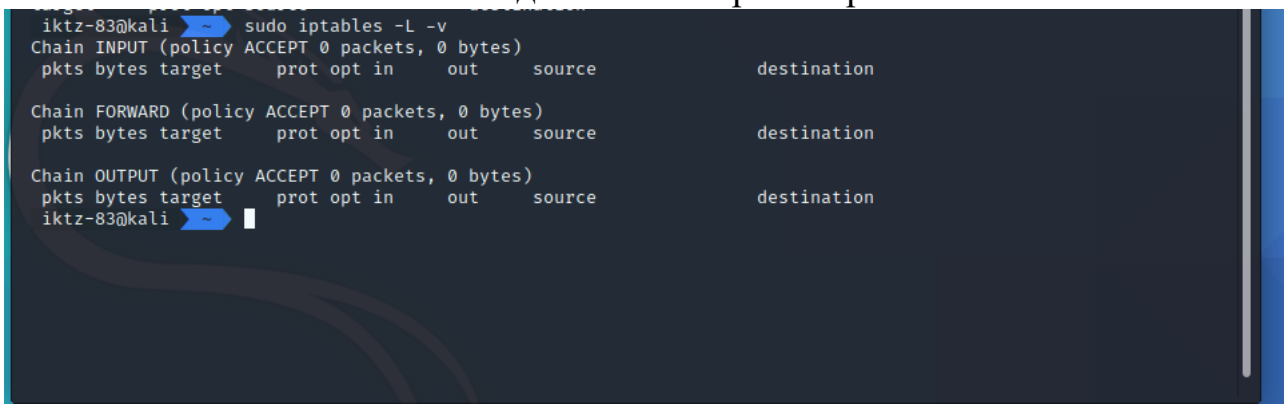

Рис. 2 Выводим список правил iptables подробнее.

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

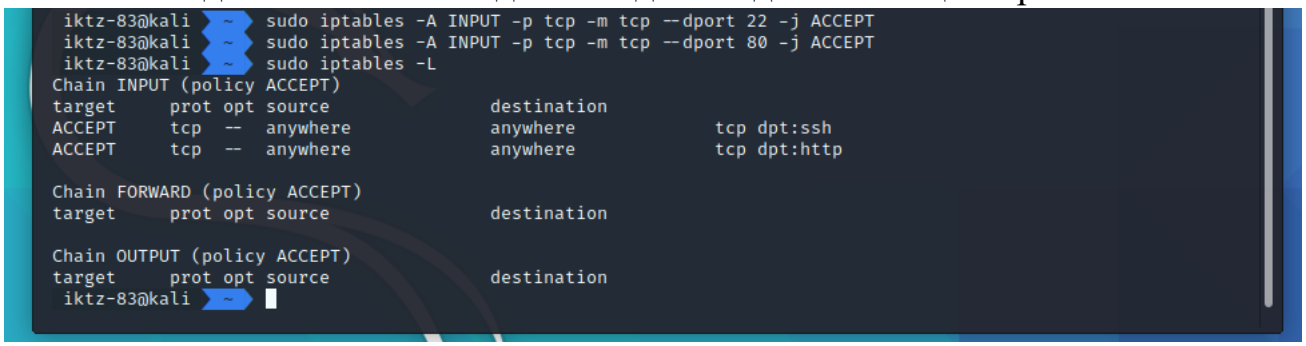

Рис. 4 Разрешаем трафик на 80 и 22 порты для tcp протокола.

```
 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

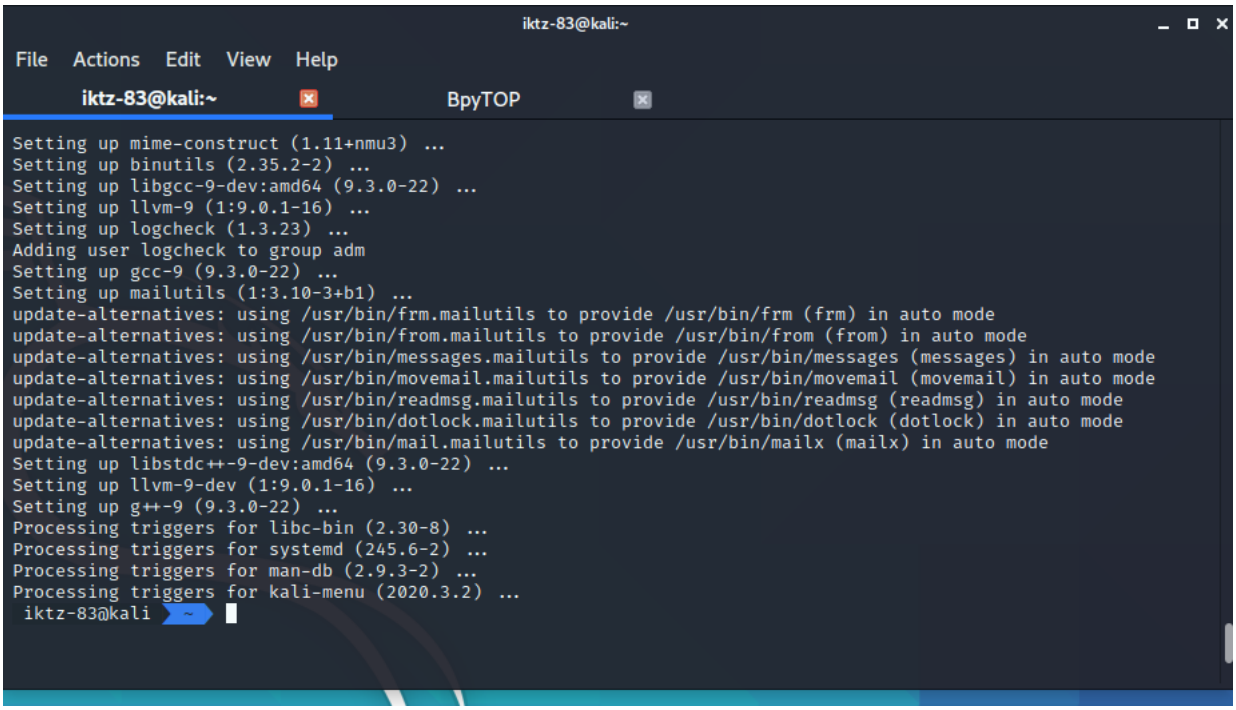

Рис. 9 logcheck успешно установлен.

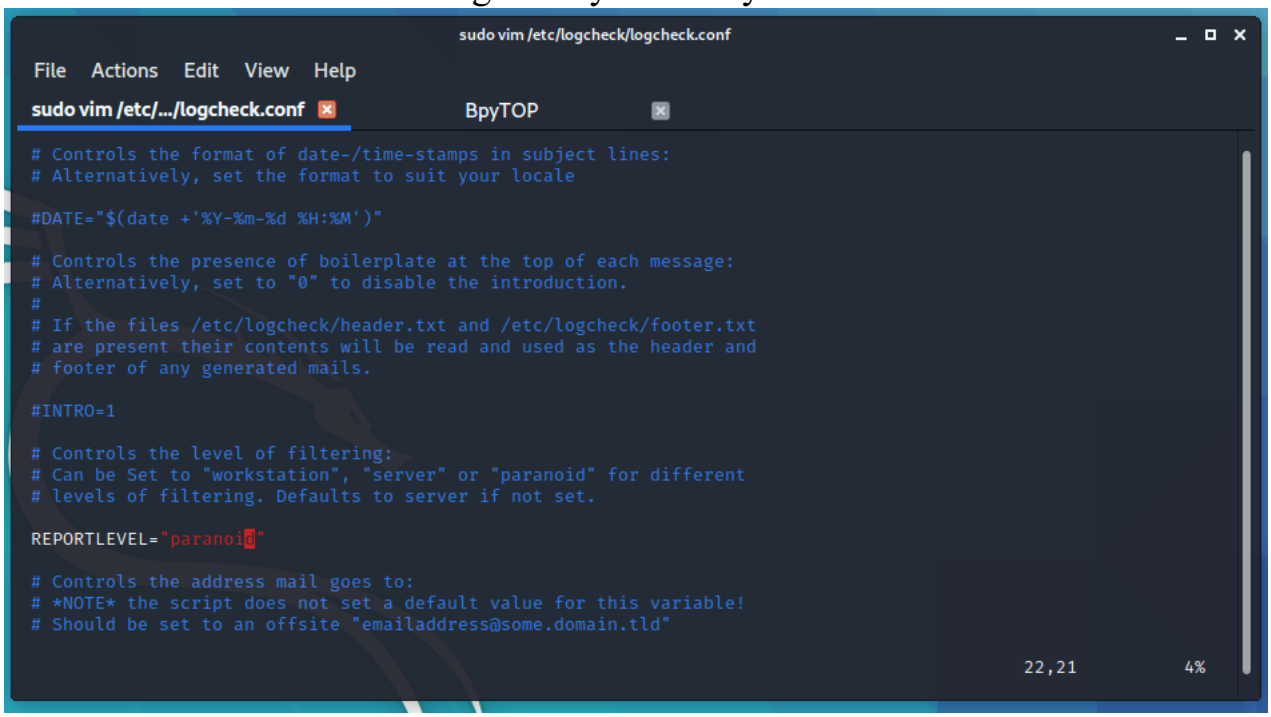

Рис. 10 Изменили REPORTLEVEL с server на paranoid

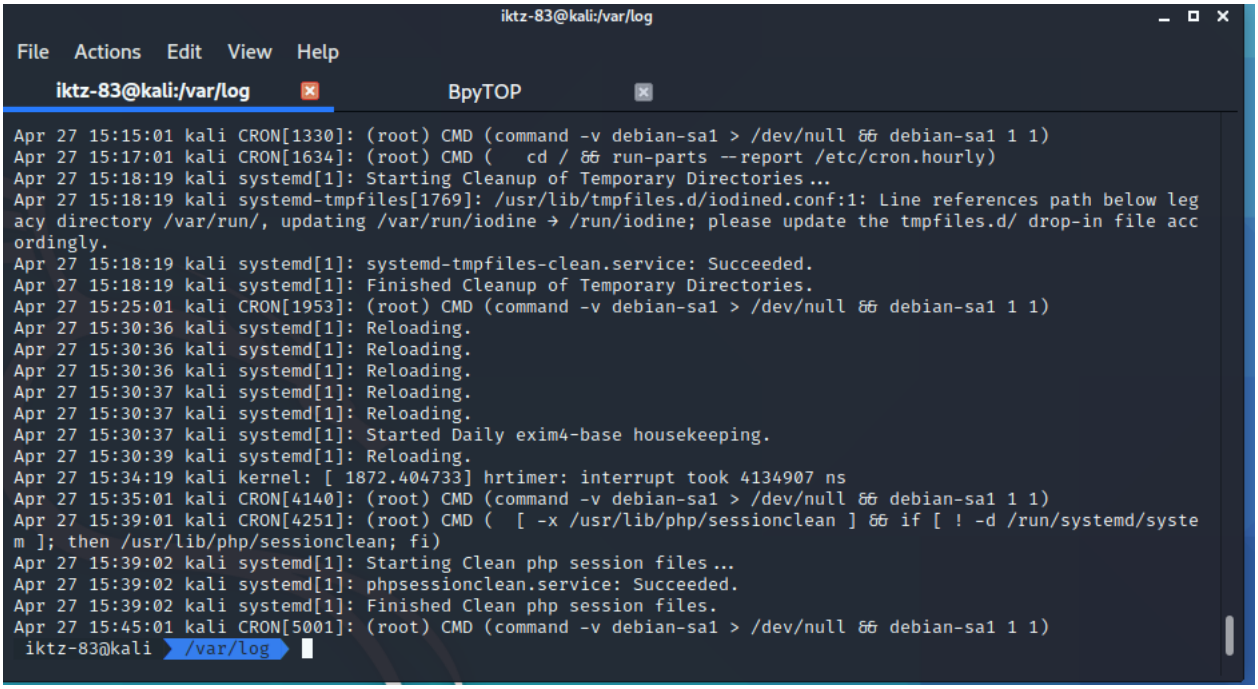

Рис. 11 Логи из файла /var/log/syslog

Часть 3 - Установка и настройка netfilter

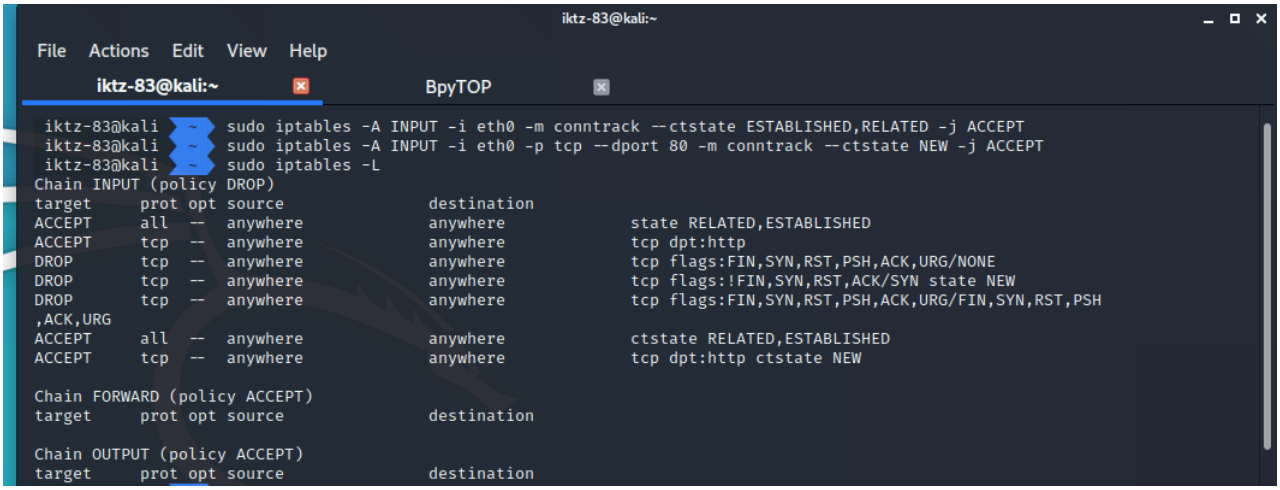

Рис. 12 Помечаем каждый пакет с помощью модуля conntrack.

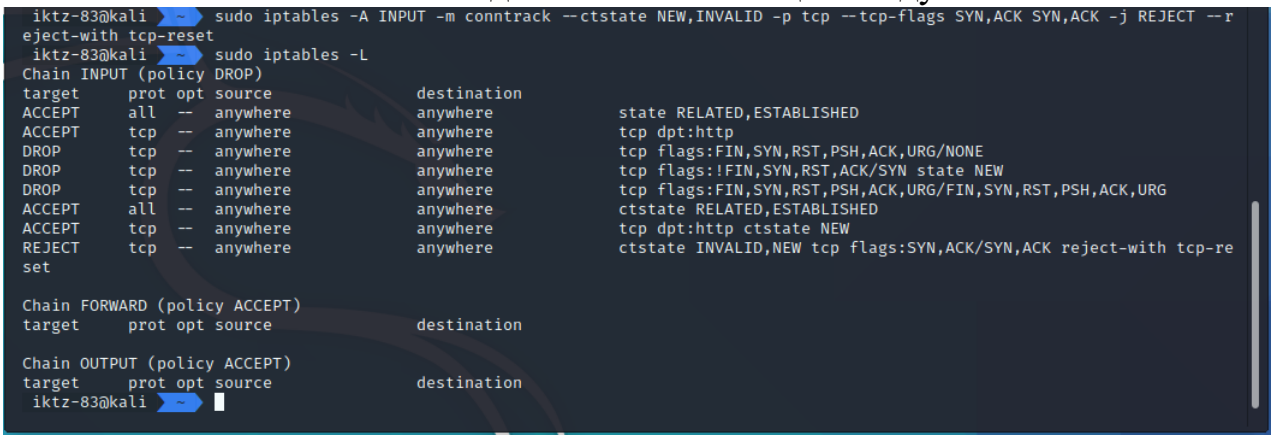

Рис. 13 Сопоставляем метки с состоянием битов.

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

```
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

Часть 6 - Установка LOIC на Kali Linux.

```
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

```
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

```
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

```
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

```
 iktz-83@kali  ~  echo "deb https://download.mono-project.com/repo/debian vs-buster main" | sudo tee /etc/apt/sources.list.d
/mono-official-vs.list
deb https://download.mono-project.com/repo/debian vs-buster main
 iktz-83@kali  ~  sudo apt update
Err:1 https://download.mono-project.com/repo/debian vs-buster InRelease
  Temporary failure resolving 'download.mono-project.com'
Err:2 http://http.kali.org/kali kali-rolling InRelease
  Temporary failure resolving 'http.kali.org'
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
1458 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  Temporary failure resolving 'http.kali.org'
W: Failed to fetch https://download.mono-project.com/repo/debian/dists/vs-buster/InRelease  Temporary failure resolving 'downl
oad.mono-project.com'
W: Some index files failed to download. They have been ignored, or old ones used instead.
 iktz-83@kali  ~
```

Рис. 20

```
File  Actions  Edit  View  Help
iktz-83@kali:~                BpyTOP
Certificate added: C=CH, O=SwissSign AG, CN=SwissSign Silver CA - G2
Certificate added: C=PL, O=Krajowa Izba Rozliczeniowa S.A., CN=SZAFIR ROOT CA2
Certificate added: C=TW, O=Government Root Certification Authority
Certificate added: O=TeliaSonera, CN=TeliaSonera Root CA v1
Certificate added: C=PA, S=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor ECA-1
Certificate added: C=PA, S=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-1
Certificate added: C=PA, S=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-2
Certificate added: C=GB, O=Trustis Limited, OU=Trustis FPS Root CA
Certificate added: C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 2
Certificate added: C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 3
Certificate added: C=TR, L=Gebze - Kocaeli, O=Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK, OU=Kamu Sertifikasyon Merkezi - Kamu SM
, CN=TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1
Certificate added: C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Global Root CA
Certificate added: C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Root Certification Authority
Certificate added: C=CN, O=UniTrust, CN=UCA Extended Validation Root
Certificate added: C=CN, O=UniTrust, CN=UCA Global G2 Root
Certificate added: C=US, S=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust ECC Certification Authority
Certificate added: C=US, S=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority
Certificate added: C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU="(c) 1999 VeriSign, Inc. - For authorized use only", CN=VeriSign Clas
s 3 Public Primary Certification Authority - G3
Certificate added: C=US, OU=www.xrampsecurity.com, O=XRamp Security Services Inc, CN=XRamp Global Certification Authority
126 new root certificates were added to your trust store.
Import process completed.
Done
done.
Processing triggers for shared-mime-info (1.15-1) ...
Setting up mono-devel (6.12.0.122-0xamarin1+debian10b1) ...
update-alternatives: using /usr/bin/mono-csc to provide /usr/bin/cli-csc (c-sharp-compiler) in auto mode
update-alternatives: using /usr/bin/resgen to provide /usr/bin/cli-resgen (resource-file-generator) in auto mode
update-alternatives: using /usr/bin/al to provide /usr/bin/cli-al (assembly-linker) in auto mode
update-alternatives: using /usr/bin/sn to provide /usr/bin/cli-sn (strong-name-tool) in auto mode
Setting up fsharp (5.0.0.0-0xamarin15+debian10b1) ...
* Installing 2 assemblies from fsharp into Mono framework paths
Setting up monodevelop (7.8.4.1-0xamarin6+debian10b1) ...
 iktz-83@kali  ~
```

Рис. 21

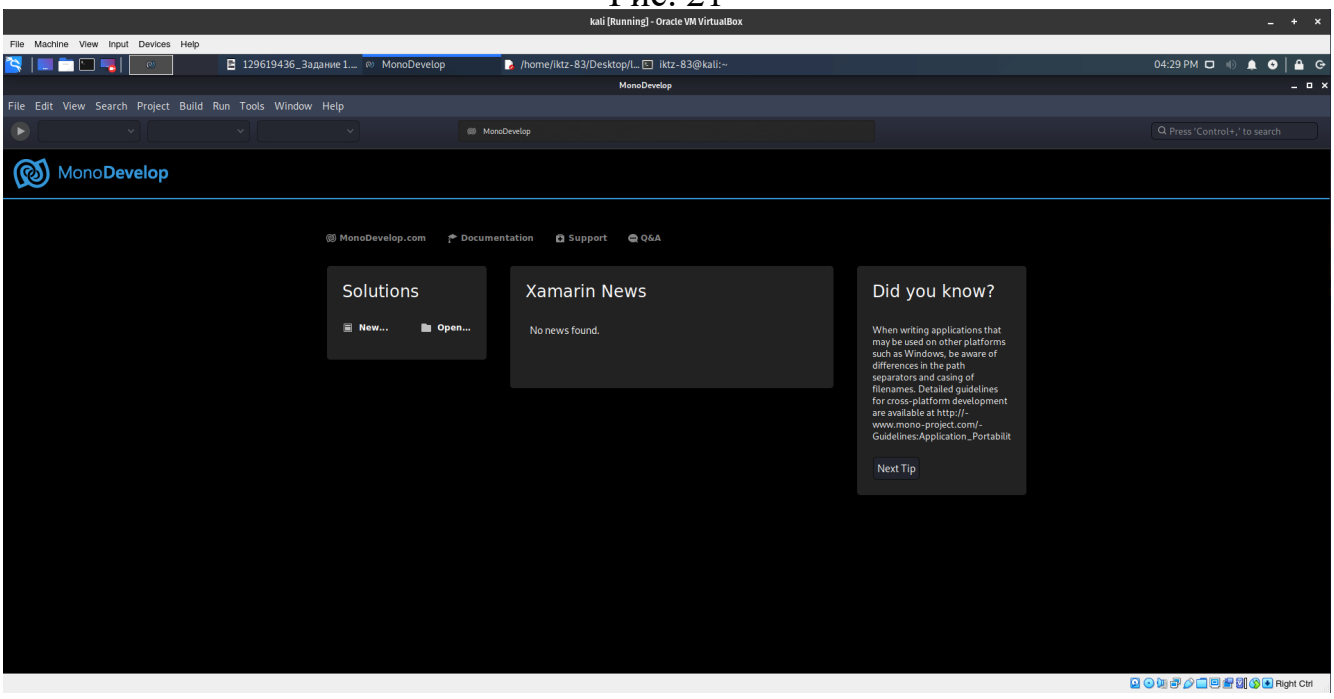

Рис. 22

```
 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

```
 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

```
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

```
 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

```
 iktz-83@kali  ~/loic  ./loic.sh update
/usr/bin/git
warning: redirecting to https://github.com/NewEraCracker/LOIC.git/
Already 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 6.12.0.122
Copyright (C) 2005-2013 Various Mono authors

Build started 4/28/2021 9:48:40 AM.
__________________________________________________
Project "/home/iktz-83/loic/LOIC/src/LOIC.sln" (default target(s)):
        Target ValidateSolutionConfiguration:
                Building solution configuration "Debug|Any CPU".
        Target Build:
                Project "/home/iktz-83/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.
                Done building project "/home/iktz-83/loic/LOIC/src/IRC/IRC.csproj".
                Project "/home/iktz-83/loic/LOIC/src/LOIC.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.
                        Target _CopyAppConfigFile:
                        Skipping target "_CopyAppConfigFile" because its outputs are up-to-date.
```

Рис. 27

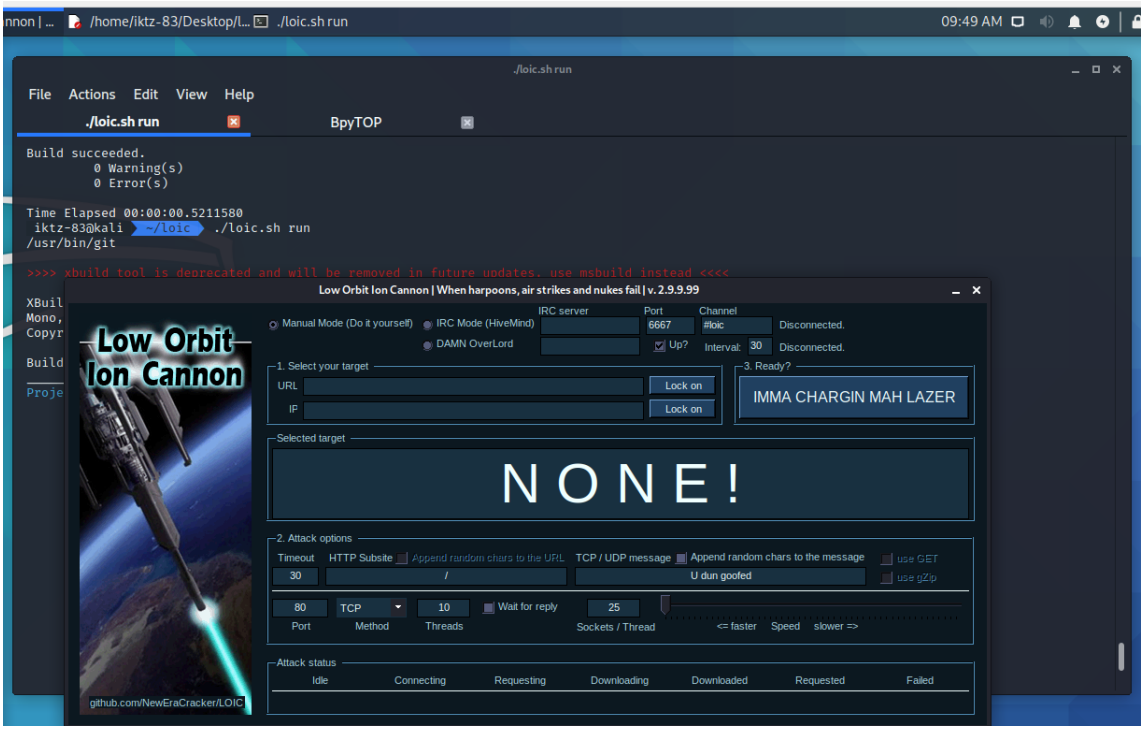

Рис. 28

Часть 7 - Установка Wifi_Jammer на Kali Linux.

Рис. 29

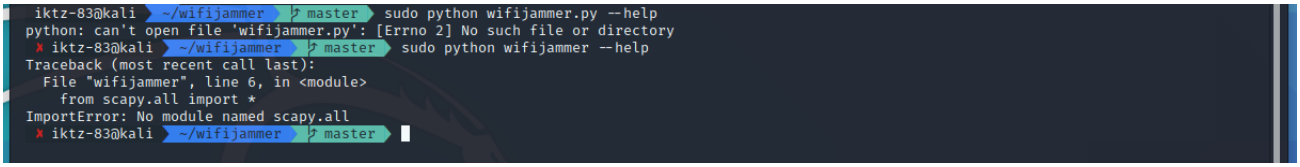

Рис. 30

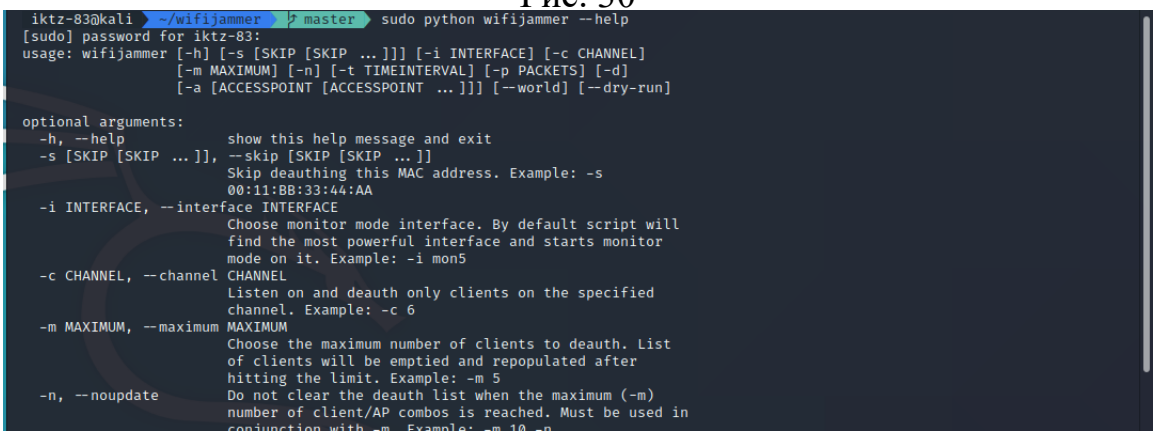

Рис. 31

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

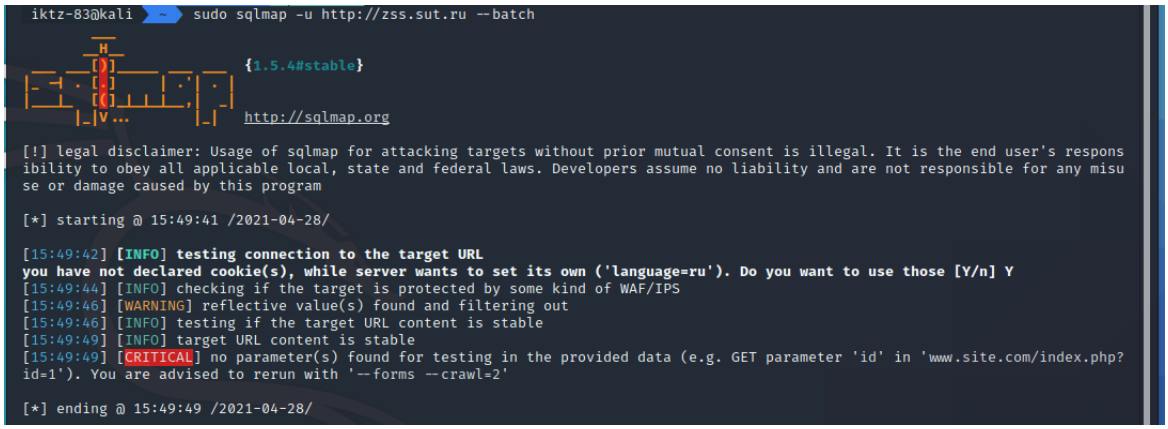

Рис. 32

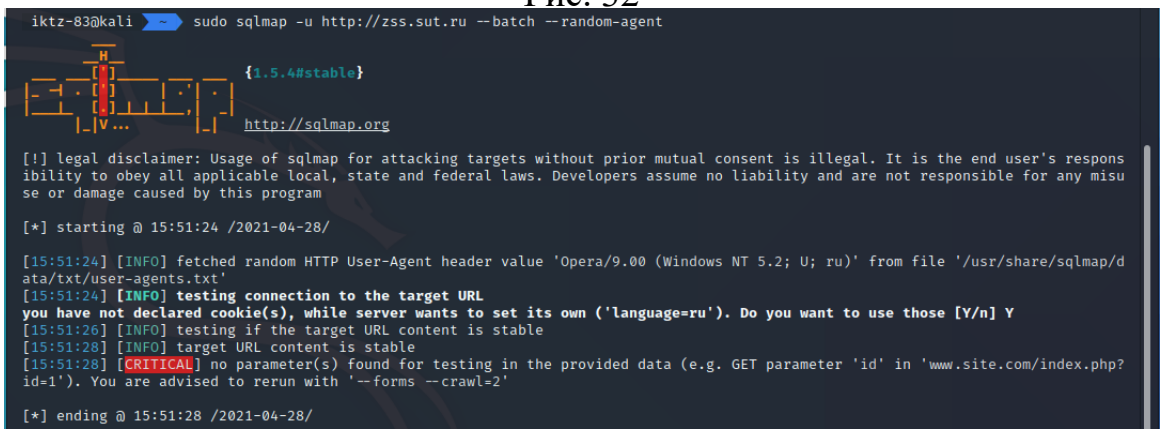

Рис. 33

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

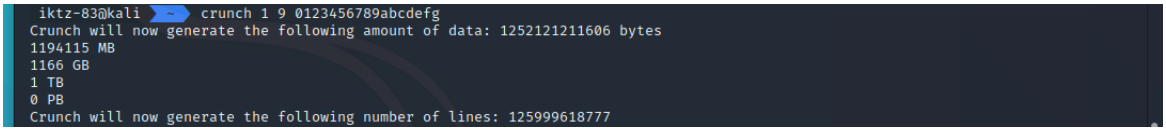

Рис. 34

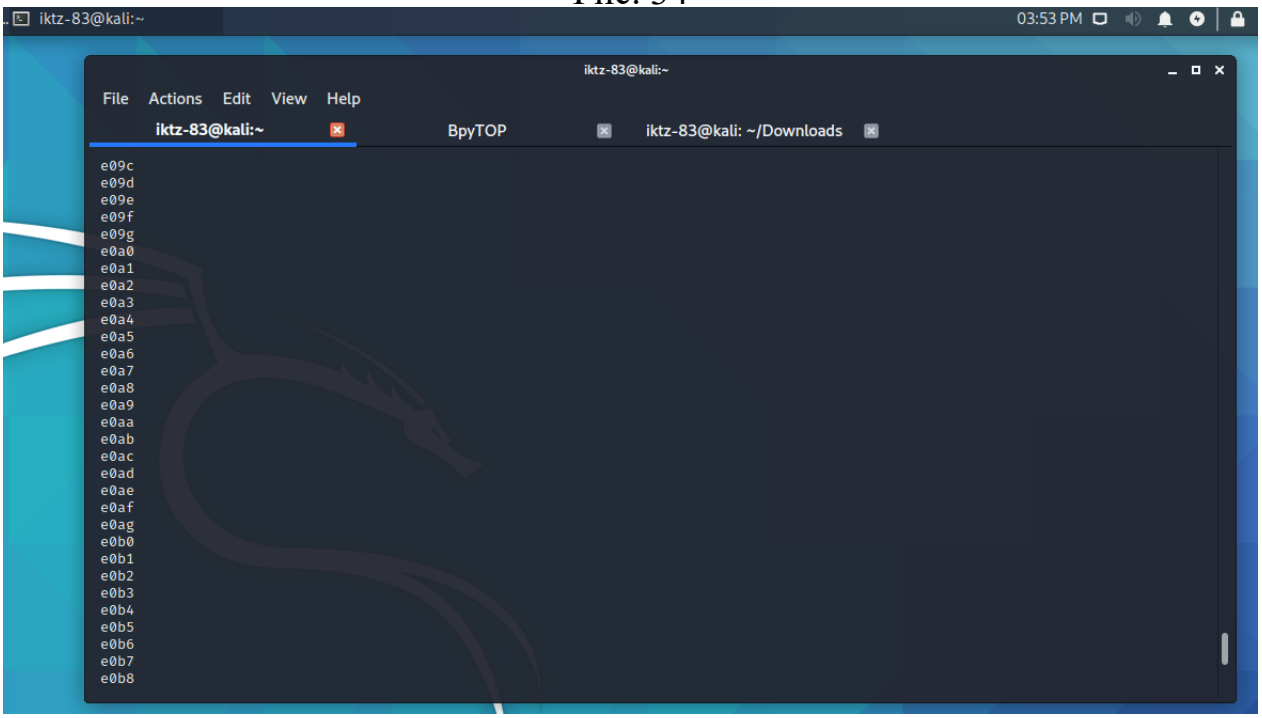

Рис. 35

Рис. 36

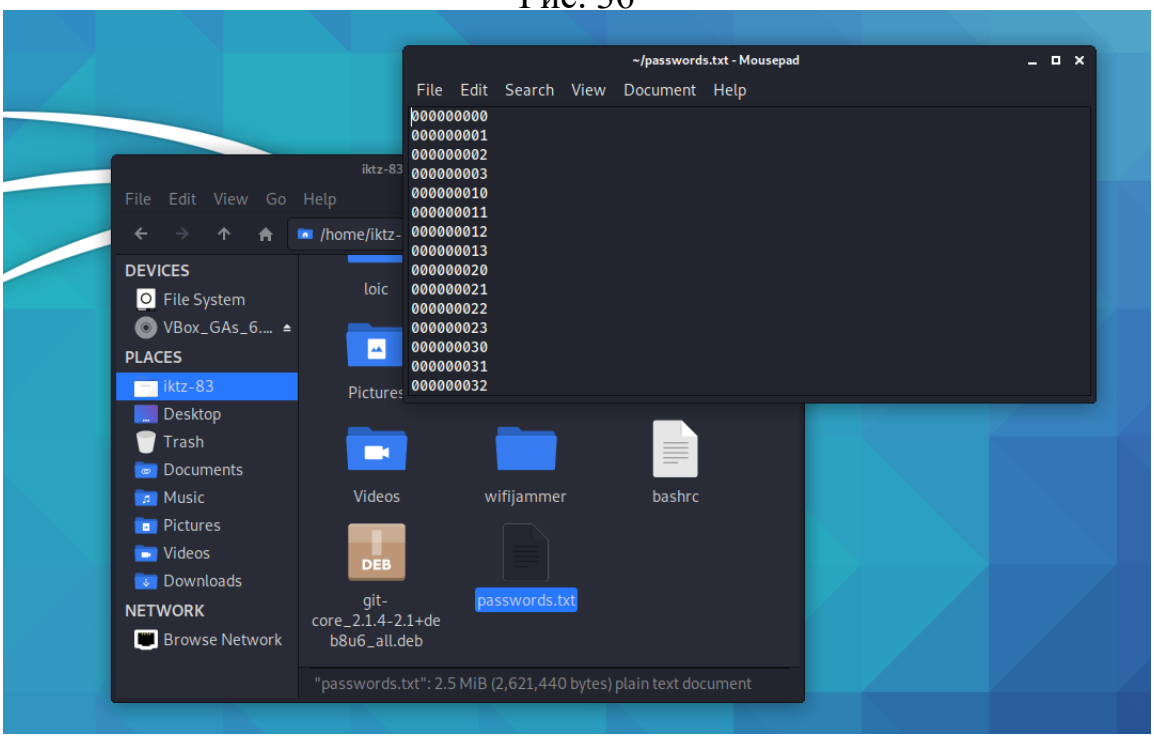

Рис. 37