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)

```
iktz-83@kali:~
File  Actions  Edit  View  Help
iktz-83@kali ~ sudo iptables -L
[sudo] password for iktz-83:
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
iktz-83@kali ~
```

Рис. 1 Выводим список правил iptables.

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

Рис. 2 Выводим список правил iptables подробнее.

```
iktz-83@kali ~ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
iktz-83@kali ~
```

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

```
iktz-83@kali ~ sudo iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
iktz-83@kali ~ sudo iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iktz-83@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
iktz-83@kali ~
```

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

```
iktz-83@kali:~
File  Actions  Edit  View  Help
iktz-83@kali:~        BpyTOP
Setting up mime-construct (1.11+nmu3) ...
Setting up binutils (2.35.2-2) ...
Setting up libgcc-9-dev:amd64 (9.3.0-22) ...
Setting up llvm-9 (1:9.0.1-16) ...
Setting up logcheck (1.3.23) ...
Adding user logcheck to group adm
Setting up gcc-9 (9.3.0-22) ...
Setting up mailutils (1:3.10-3+b1) ...
update-alternatives: using /usr/bin/frm.mailutils to provide /usr/bin/frm (frm) in auto mode
update-alternatives: using /usr/bin/from.mailutils to provide /usr/bin/from (from) in auto mode
update-alternatives: using /usr/bin/messages.mailutils to provide /usr/bin/messages (messages) in auto mode
update-alternatives: using /usr/bin/movemail.mailutils to provide /usr/bin/movemail (movemail) in auto mode
update-alternatives: using /usr/bin/readmsg.mailutils to provide /usr/bin/readmsg (readmsg) in auto mode
update-alternatives: using /usr/bin/dotlock.mailutils to provide /usr/bin/dotlock (dotlock) in auto mode
update-alternatives: using /usr/bin/mail.mailutils to provide /usr/bin/mailx (mailx) in auto mode
Setting up libstdc++-9-dev:amd64 (9.3.0-22) ...
Setting up llvm-9-dev (1:9.0.1-16) ...
Setting up g++-9 (9.3.0-22) ...
Processing triggers for libc-bin (2.30-8) ...
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. 9 logcheck успешно установлен.

```
sudo vim /etc/logcheck/logcheck.conf
File  Actions  Edit  View  Help
sudo vim /etc/.../logcheck.conf        BpyTOP
# 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="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"

                                                          22,21          4%
```

Рис. 10 Изменили REPORTLEVEL с server на paranoid.

```
iktz-83@kali:/var/log
File  Actions  Edit  View  Help
iktz-83@kali:/var/log        BpyTOP

Apr 27 15:15:01 kali CRON[1330]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Apr 27 15:17:01 kali CRON[1634]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Apr 27 15:18:19 kali systemd[1]: Starting Cleanup of Temporary Directories...
Apr 27 15:18:19 kali systemd-tmpfiles[1769]: /usr/lib/tmpfiles.d/iodined.conf:1: Line references path below leg
acy directory /var/run/, updating /var/run/iodine → /run/iodine; please update the tmpfiles.d/ drop-in file acc
ordingly.
Apr 27 15:18:19 kali systemd[1]: systemd-tmpfiles-clean.service: Succeeded.
Apr 27 15:18:19 kali systemd[1]: Finished Cleanup of Temporary Directories.
Apr 27 15:25:01 kali CRON[1953]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Apr 27 15:30:36 kali systemd[1]: Reloading.
Apr 27 15:30:36 kali systemd[1]: Reloading.
Apr 27 15:30:36 kali systemd[1]: Reloading.
Apr 27 15:30:37 kali systemd[1]: Reloading.
Apr 27 15:30:37 kali systemd[1]: Reloading.
Apr 27 15:30:37 kali systemd[1]: Started Daily exim4-base housekeeping.
Apr 27 15:30:39 kali systemd[1]: Reloading.
Apr 27 15:34:19 kali kernel: [ 1872.404733] hrtimer: interrupt took 4134907 ns
Apr 27 15:35:01 kali CRON[4140]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Apr 27 15:39:01 kali CRON[4251]: (root) CMD (  [ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/syste
m ]; then /usr/lib/php/sessionclean; fi)
Apr 27 15:39:02 kali systemd[1]: Starting Clean php session files...
Apr 27 15:39:02 kali systemd[1]: phpsessionclean.service: Succeeded.
Apr 27 15:39:02 kali systemd[1]: Finished Clean php session files.
Apr 27 15:45:01 kali CRON[5001]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
 iktz-83@kali  /var/log
```

Рис. 11 Логи из файла /var/log/syslog.

Часть 3 - Установка и настройка netfilter

```
iktz-83@kali:~
File  Actions  Edit  View  Help
iktz-83@kali:~        BpyTOP

 iktz-83@kali  ~  sudo iptables -A INPUT -i eth0 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
 iktz-83@kali  ~  sudo iptables -A INPUT -i eth0 -p tcp --dport 80 -m conntrack --ctstate NEW -j ACCEPT
 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
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http ctstate NEW

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

Рис. 12 Помечаем каждый пакет с помощью модуля conntrack.

```
 iktz-83@kali  ~  sudo iptables -A INPUT -m conntrack --ctstate NEW,INVALID -p tcp --tcp-flags SYN,ACK SYN,ACK -j REJECT --r
eject-with tcp-reset
 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
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http ctstate NEW
REJECT     tcp  --  anywhere             anywhere             ctstate INVALID,NEW tcp flags:SYN,ACK/SYN,ACK reject-with tcp-re
set

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
 iktz-83@kali  ~
```

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.

```
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.

```
✘ 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.

```
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 Команда для установки MonoDevelop.

```
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 (6.12.0.122-0×amarin1+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 (5.0.0.0-0×amarin15+debian10b1) ...
* Installing 2 assemblies from fsharp into Mono framework paths
Setting up monodevelop (7.8.4.1-0×amarin6+debian10b1) ...
iktz-83@kali ~
```

Рис. 21 Команда для установки MonoDevelop.

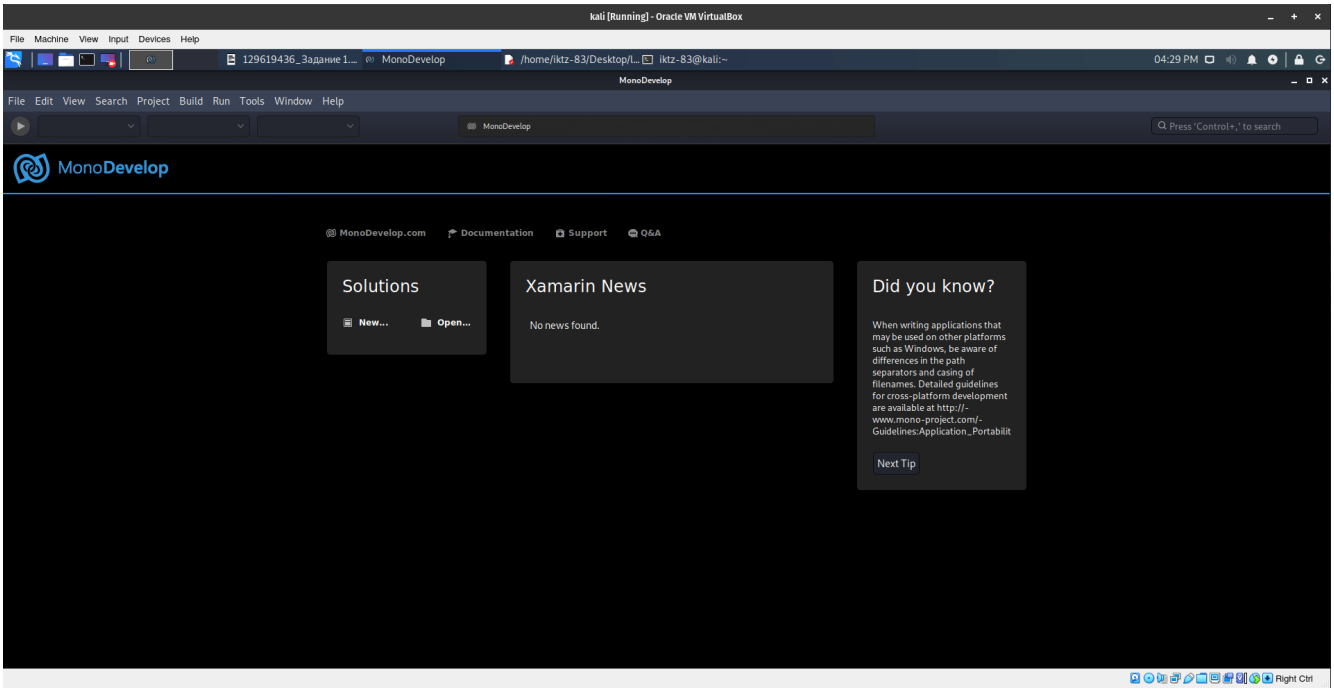

Рис. 22 Интерфейс программы MonoDevelop.

```
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.

```
 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 Обновляем.

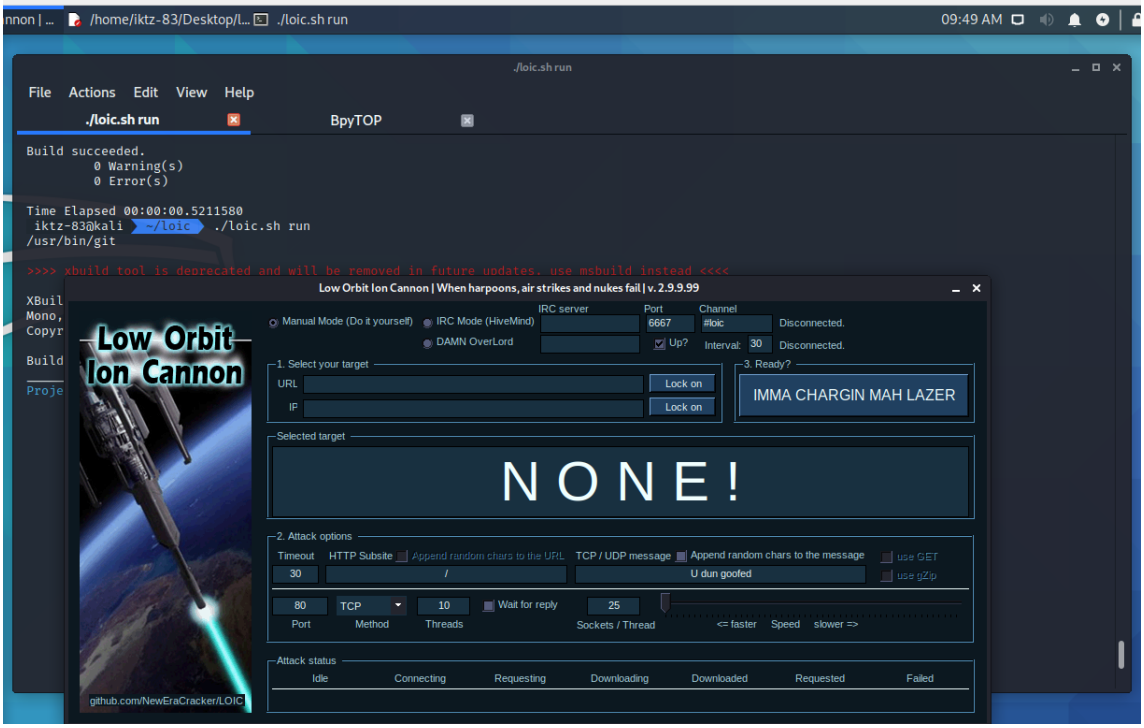

Рис. 28 Программа loic установленна, и запущена.

Часть 7 - Установка Wifi_Jammer на Kali Linux.

```
iktz-83@kali:~/wifijammer
File  Actions  Edit  View  Help
iktz-83@kali:~/wifijammer        BpyTOP

iktz-83@kali  ~  git clone https://github.com/DanMcInerney/wifijammer.git
Cloning into 'wifijammer'...
remote: Enumerating objects: 274, done.
remote: Total 274 (delta 0), reused 0 (delta 0), pack-reused 274
Receiving objects: 100% (274/274), 82.17 KiB | 1.05 MiB/s, done.
Resolving deltas: 100% (111/111), done.
iktz-83@kali  ~  cd wifijammer
iktz-83@kali  ~/wifijammer  master
```

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

```
iktz-83@kali  ~/wifijammer  master  sudo python wifijammer.py --help
python: can't open file 'wifijammer.py': [Errno 2] No such file or directory
✘ iktz-83@kali  ~/wifijammer  master  sudo python wifijammer --help
Traceback (most recent call last):
  File "wifijammer", line 6, in <module>
    from scapy.all import *
ImportError: No module named scapy.all
✘ iktz-83@kali  ~/wifijammer  master
```

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

```
iktz-83@kali  ~/wifijammer  master  sudo python wifijammer --help
[sudo] password for iktz-83:
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
```

Рис. 31 wifijammer работает, после установки недостающего пакета.

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

```
iktz-83@kali  ~  sudo sqlmap -u http://zss.sut.ru --batch
                 {1.5.4#stable}
                 http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's respons
ibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misu
se or damage caused by this program

[*] starting @ 15:49:41 /2021-04-28/

[15:49:42] [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
[15:49:44] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:49:46] [WARNING] reflective value(s) found and filtering out
[15:49:46] [INFO] testing if the target URL content is stable
[15:49:49] [INFO] target URL content is stable
[15:49:49] [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 @ 15:49:49 /2021-04-28/
```

Рис. 32 Производим SQL-инъекцию со стандартным поведением.

```
iktz-83@kali ~ sudo sqlmap -u http://zss.sut.ru --batch --random-agent
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's respons
ibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misu
se or damage caused by this program

[*] starting @ 15:51:24 /2021-04-28/

[15:51:24] [INFO] fetched random HTTP User-Agent header value 'Opera/9.00 (Windows NT 5.2; U; ru)' from file '/usr/share/sqlmap/d
ata/txt/user-agents.txt'
[15:51:24] [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
[15:51:26] [INFO] testing if the target URL content is stable
[15:51:28] [INFO] target URL content is stable
[15:51:28] [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 @ 15:51:28 /2021-04-28/
```

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.

```
iktz-83@kali:~                                                    03:53 PM
iktz-83@kali:~
File  Actions  Edit  View  Help
iktz-83@kali:~   BpyTOP   iktz-83@kali: ~/Downloads
e09c
e09d
e09e
e09f
e09g
e0a0
e0a1
e0a2
e0a3
e0a4
e0a5
e0a6
e0a7
e0a8
e0a9
e0aa
e0ab
e0ac
e0ad
e0ae
e0af
e0ag
e0b0
e0b1
e0b2
e0b3
e0b4
e0b5
e0b6
e0b7
e0b8
```

Рис. 35 Пример паролей.

```
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.

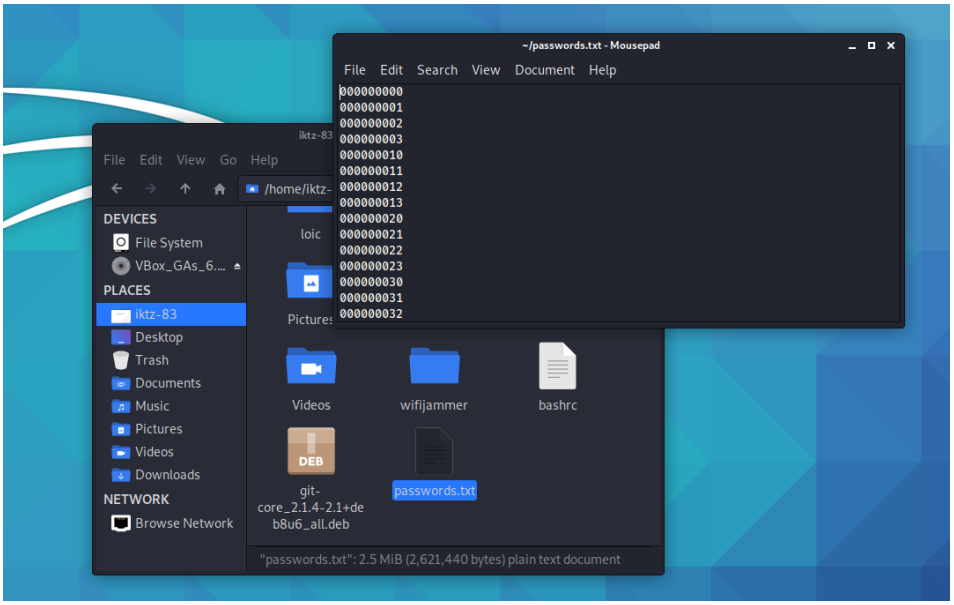

Рис. 37 Проверяем файл passwords.txt.

Вывод

В ходе данной лабораторной работы мы научились настраивать стандартный файервол linux - iptables. Также установили мониторинг журналов logcheck и произвели его настройку. Установили программы MonoDevelop, Loic и wifijammer. Сделали попытку совершить SQL-инъекцию на сайт zss.sut.ru, и изучили работу консольной программы crunch.