



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»
РТУ МИРЭА

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

Отчет по практической работе №7
по дисциплине: «Управление информационной безопасностью»

Выполнила:
Студентка группы ББМО-02-22
Бардасова И.А.

Проверил:
Пимонов Р.В.

Москва, 2023

Содержание

Введение	3
1 Развёртывание и настройка	4
Шаг 1. Установка Kali Linux	4
Шаг 2. Установка Damn Vulnerable Linux	4
2 Анализ защищённости	12
2.1 Сканирование сети и уязвимостей	12
Шаг 3. Инструмент OpenVas	12
Шаг 4. Инструмент Nmap	21
3 Анализ безопасности системы	24
3.1 Инструмент Metasploit	24
Заключение	29

Введение

Цель работы: Провести активное тестирование защищенности информационных систем. Развернуть две ВМ.

Задачи:

- сканирование сети с помощью Nmap;
- сканирование сети с помощью OpenVAS;
- анализ безопасности системы с помощью Metasploit.

1 Развёртывание и настройка

Шаг 1. Установка Kali Linux

Kali уже был установлен заранее, представлен на рисунке 1.

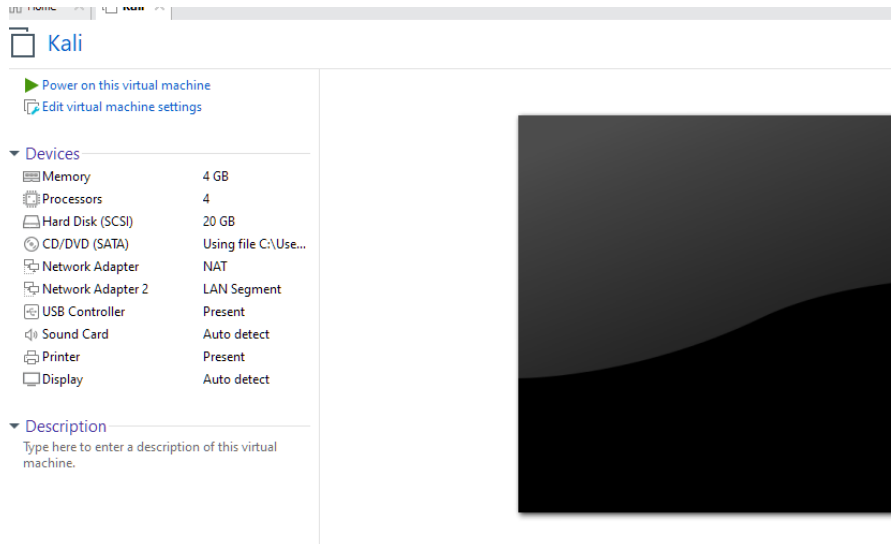


Рисунок 1 – Kali Linux

Шаг 2. Установка Damn Vulnerable Linux

Установка DVL на отдельной виртуальной машине, настройка для тестирования безопасности.

Скачаем DVL образ диска и выполним установку образа в VMWare (рис. 2).

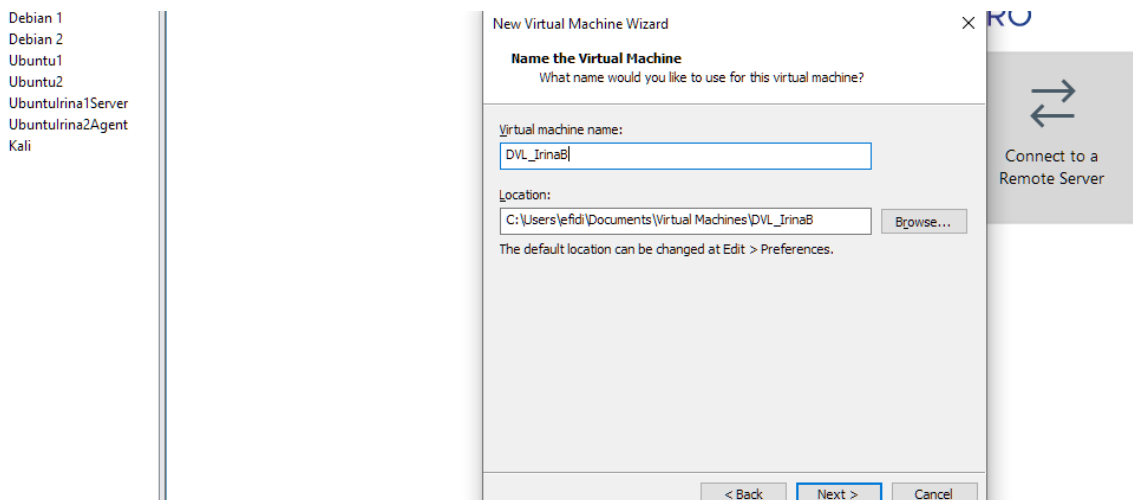


Рисунок 2 – Установка образа

Выполняется загрузка ВМ.

Теперь выполним авторизацию (рис. 3):

Логин: root

Пароль: toor

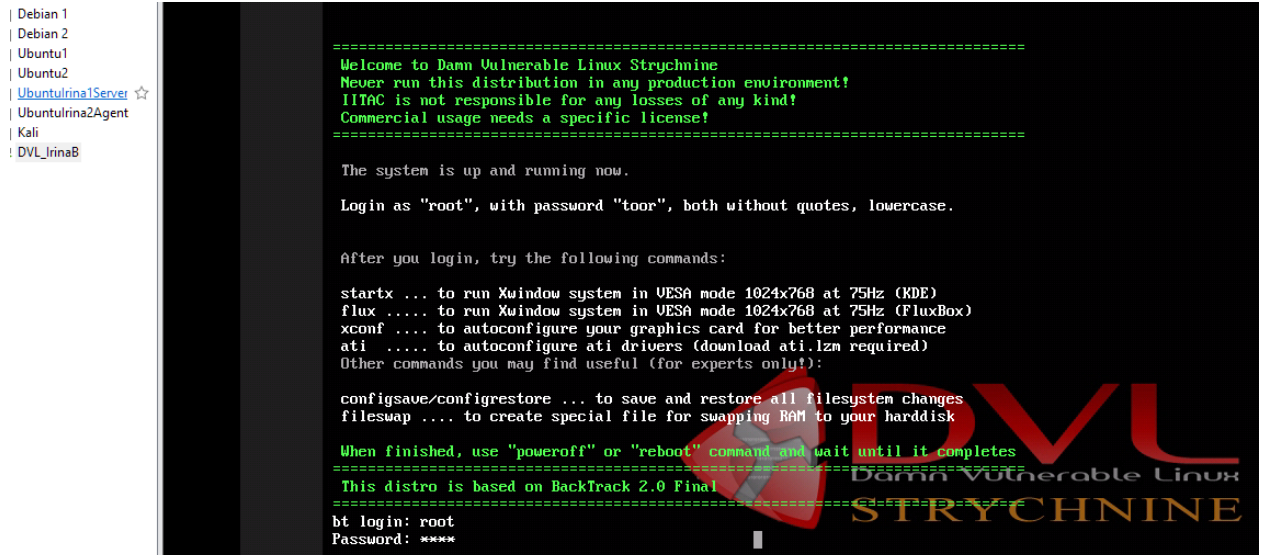


Рисунок 3 – Авторизация

Определим, какой диск форматировать (/dev/sda) (рис. 4).

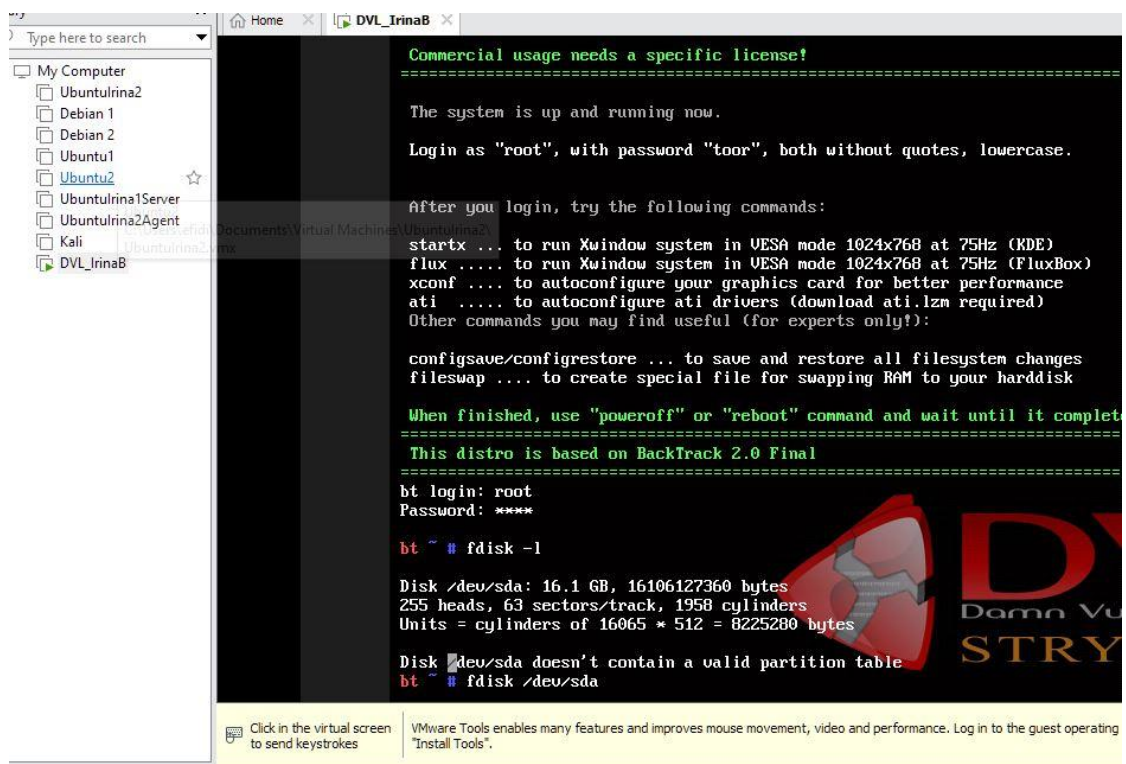


Рисунок 4 – Диск (/dev/sda)

Выберем диск для разбиения на разделы (рис. 5).

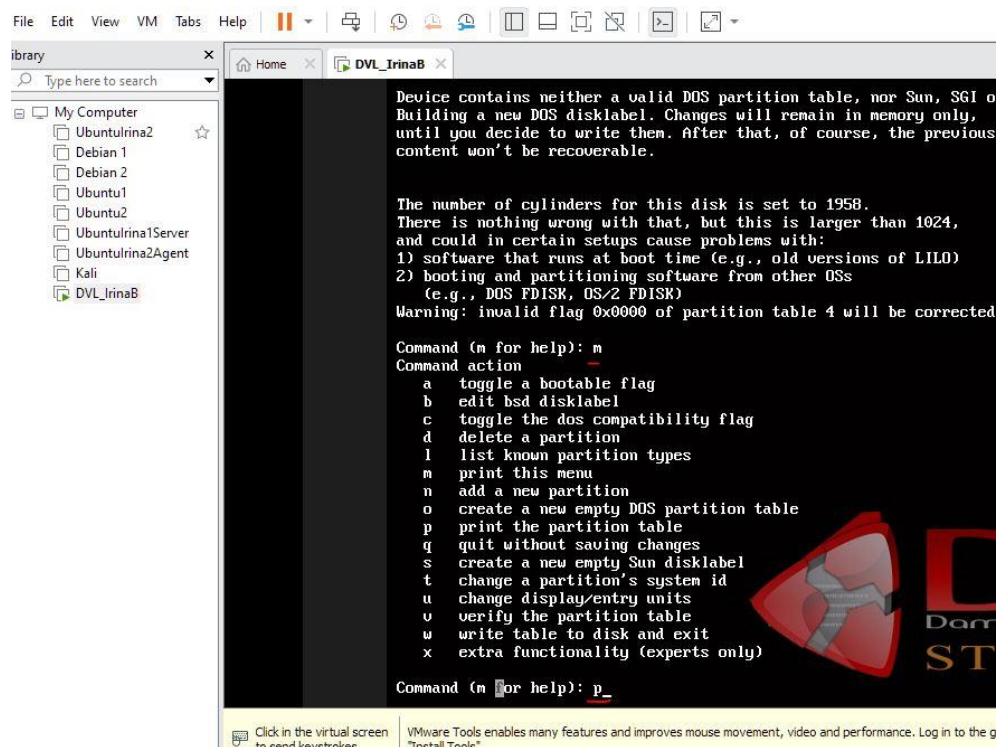


Рисунок 5 – Диск для разбиения

Посмотрим таблицу разделов. Имеется 1958 цилиндра (рис. 6).

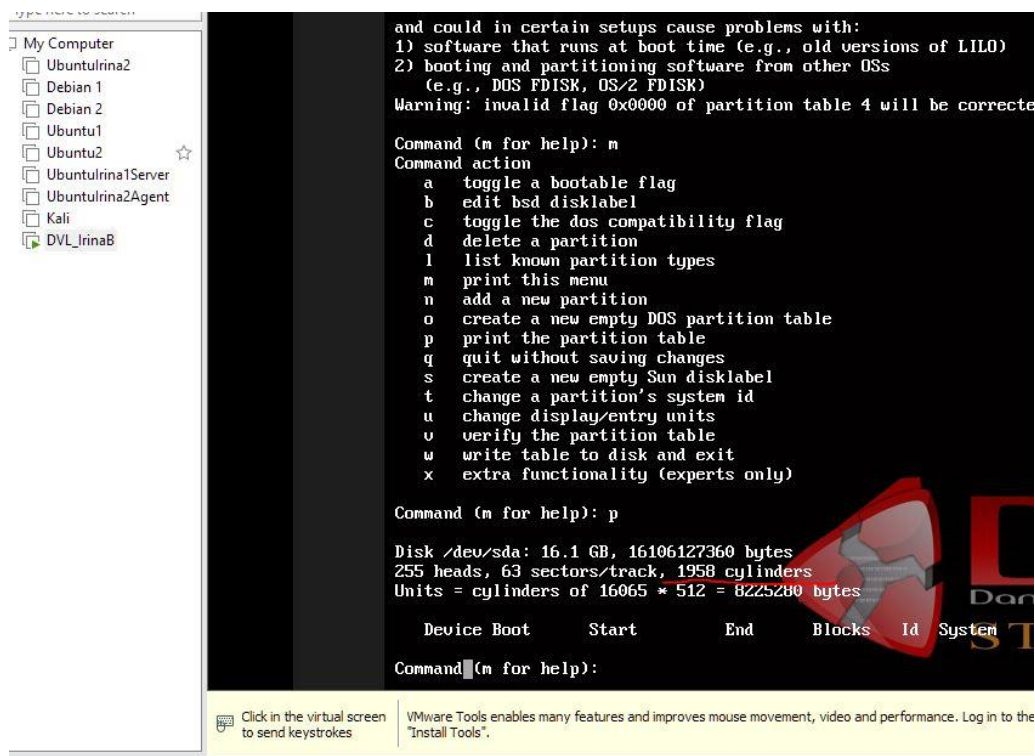


Рисунок 6 – Таблица разделов

Добавим новый раздел (рис. 7).

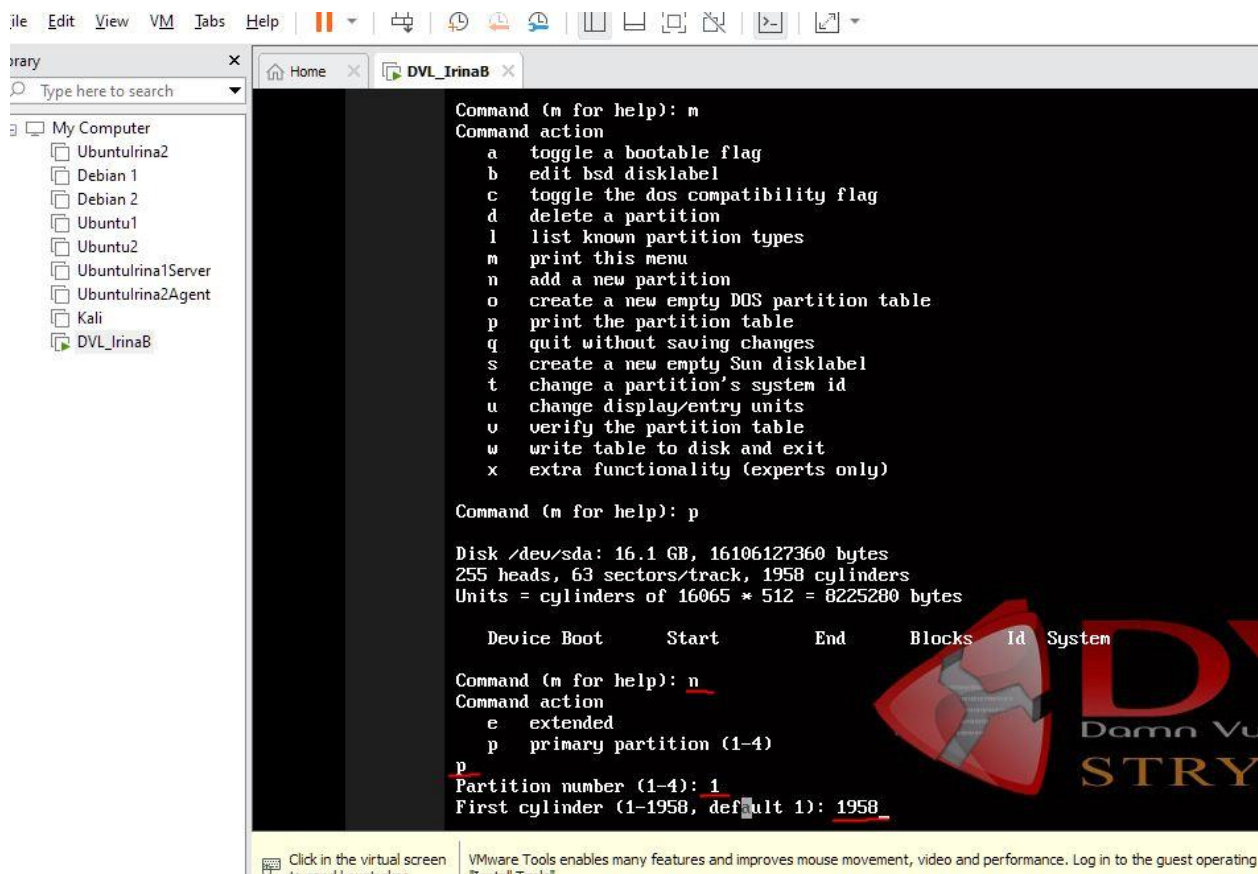


Рисунок 7 – Добавление раздела

Посмотрим на созданный раздел (рис. 8).

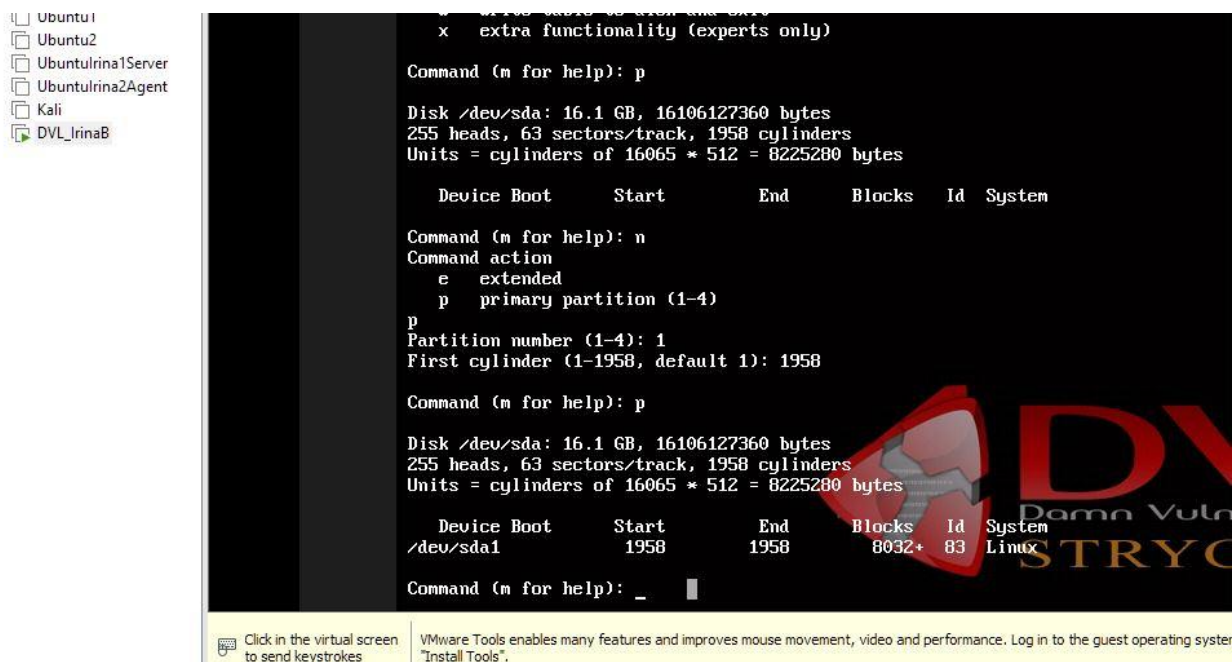


Рисунок 8 – Созданный раздел

Сохраним новый раздел и отформатируем раздел /dev/sda (рис. 9).

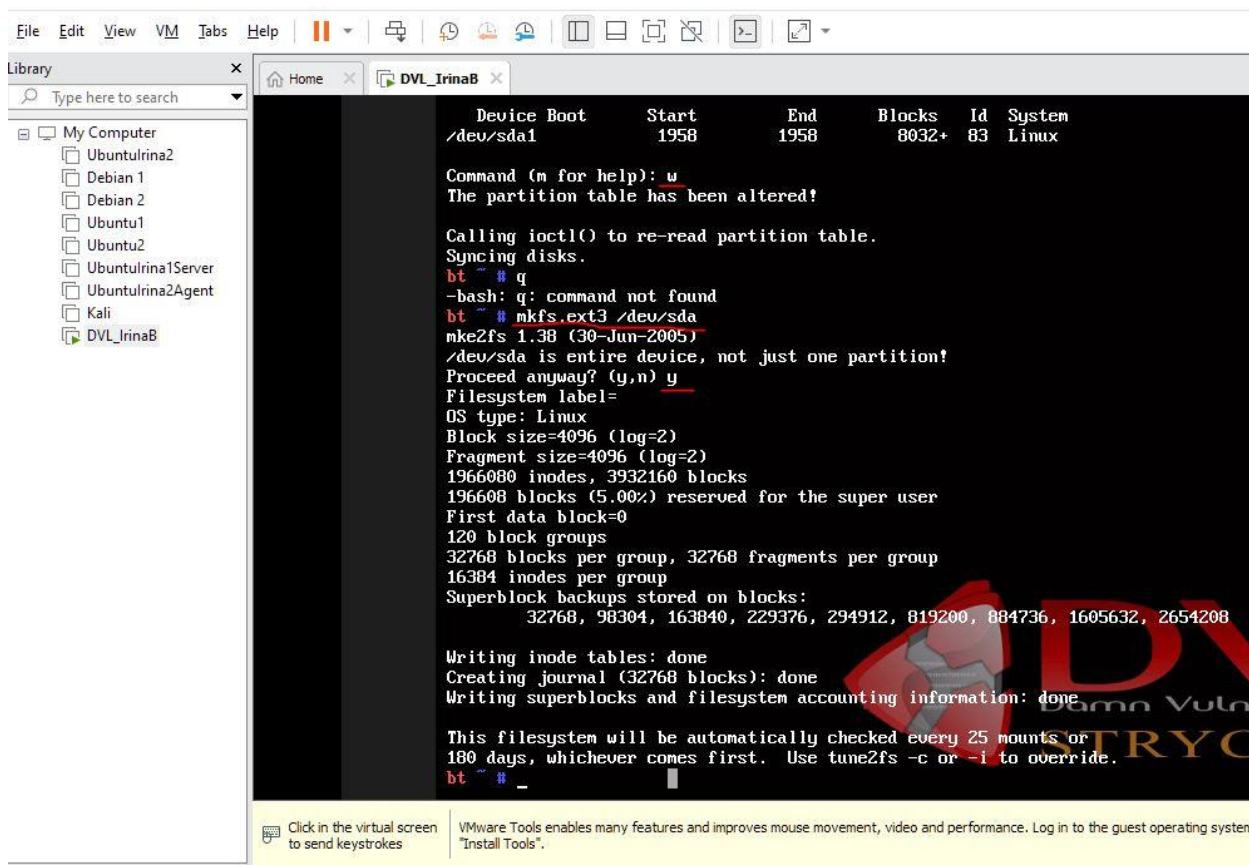


Рисунок 9 – Сохранение раздела

Создадим папку для монтирования раздела. Подключим жесткий диск к каталогу /mnt/dvl. Выполним перезагрузку (рис. 10).

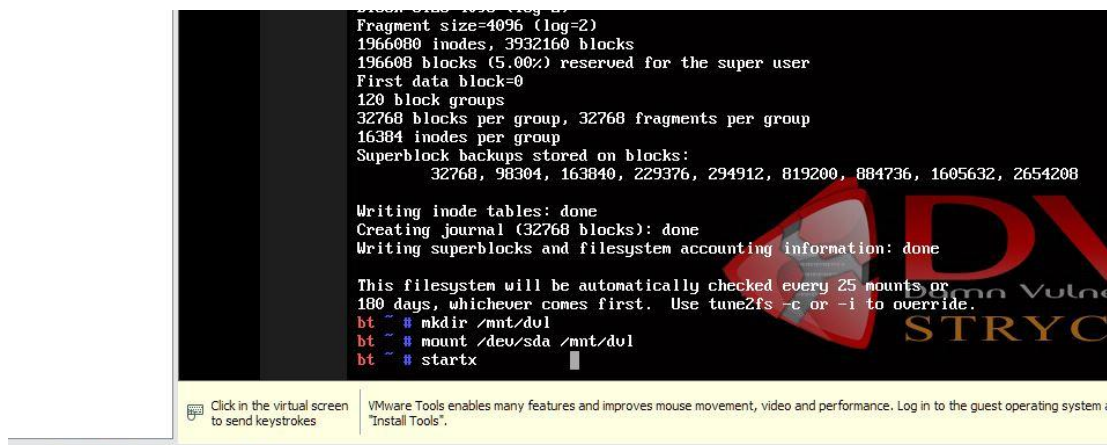


Рисунок 10 – Папка для монтирования раздела, перезагрузка

Настроим установщик BackTrack (рис. 11).

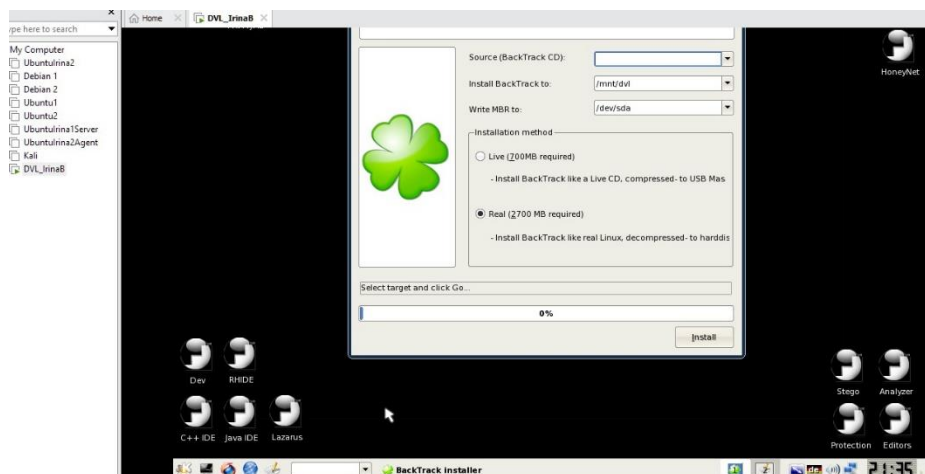


Рисунок 11 – Установщик BackTrack

Ждём завершения (рис. 12).

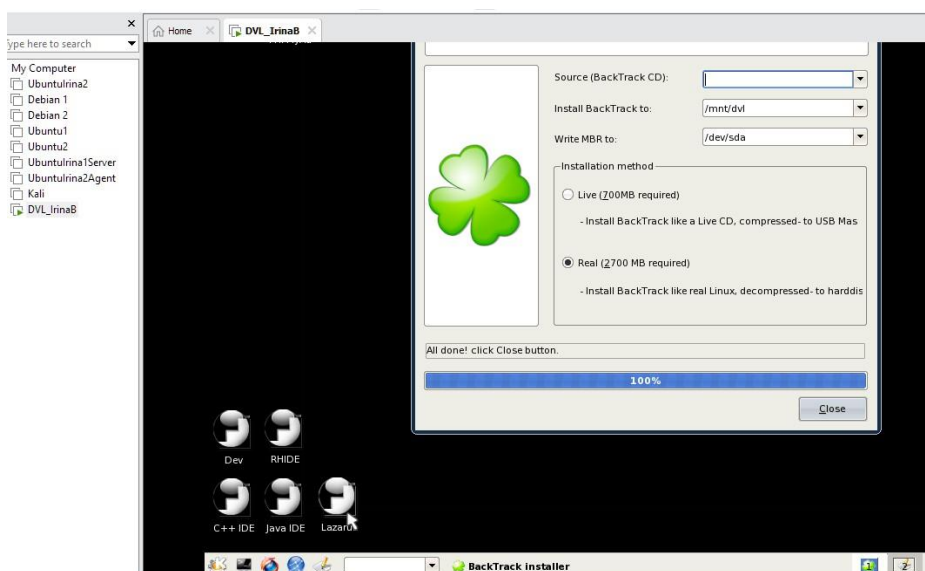


Рисунок 12 – Установщик BackTrack, выполнение

Установим загрузчик (рис. 13).

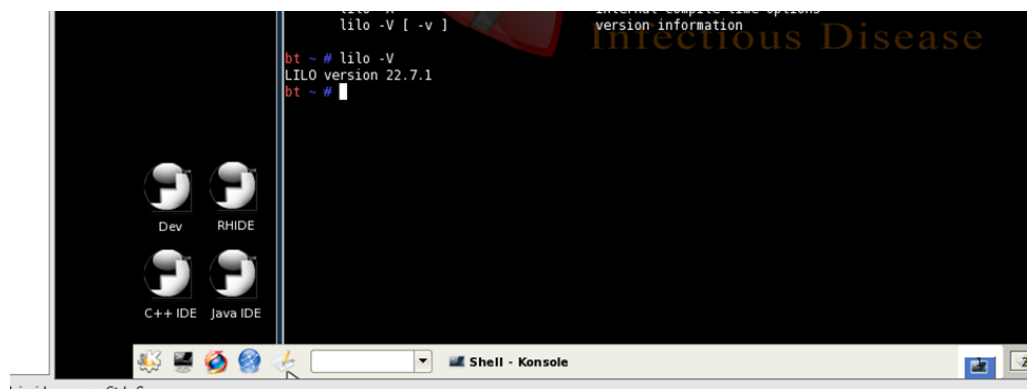


Рисунок 13 – Загрузчик

Наши готовые ВМ (рис. 14-15):

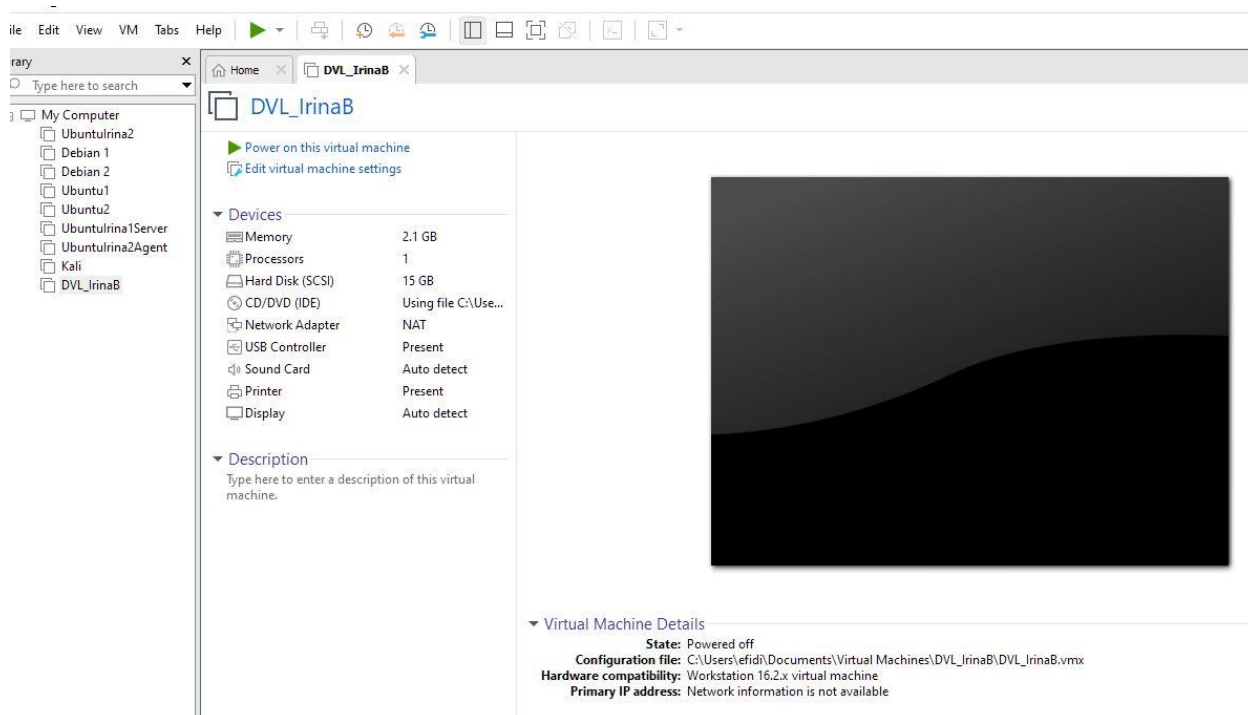


Рисунок 14 – DVL_IrinaB

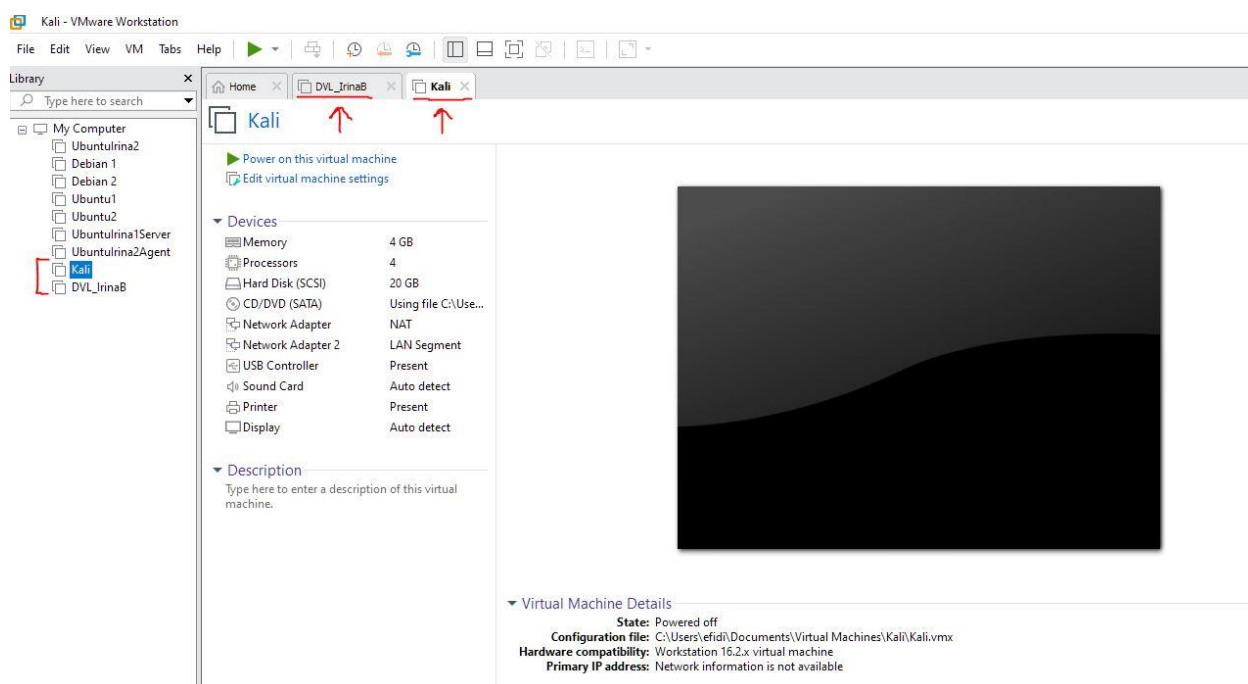


Рисунок 15 – Kali Linux

Узнаем ip-адреса и проверим связь между ними (рис. 16-17):

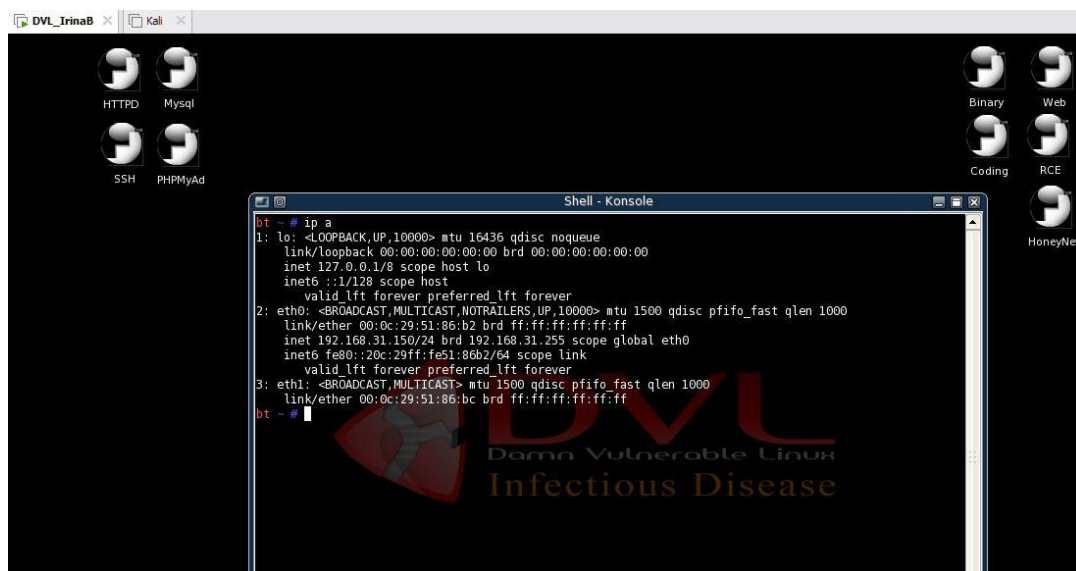


Рисунок 16 – Ip-адрес DVL

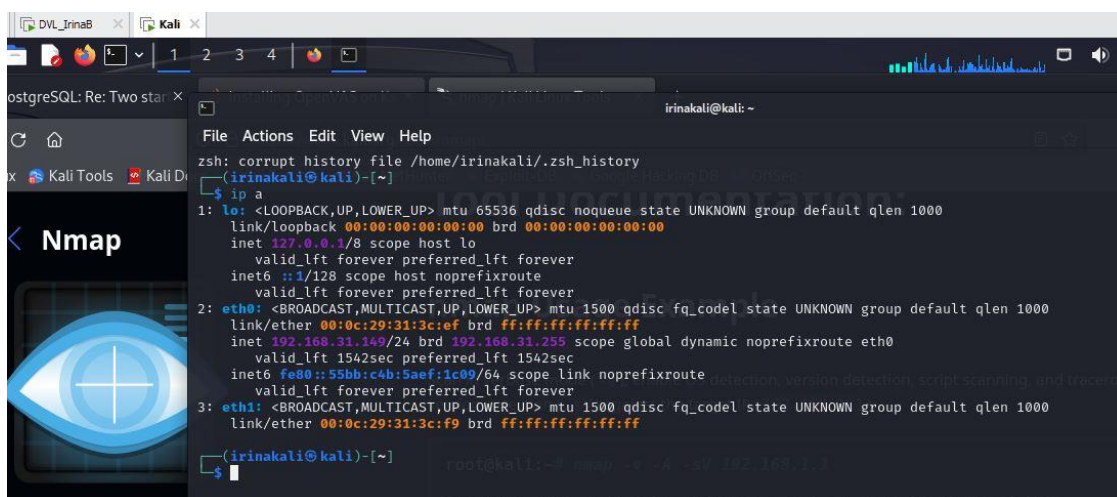


Рисунок 17 – Ip-адрес Kali

Отообразим доступность узлов друг для друга командой ping (рис. 18-19).

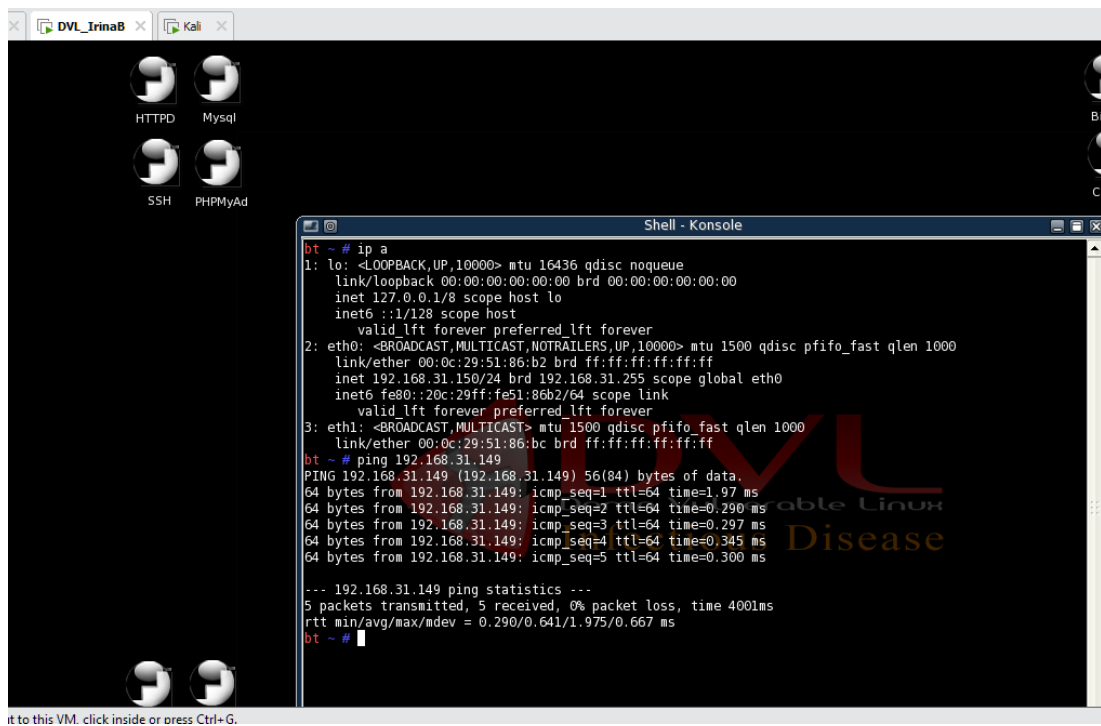


Рисунок 18 – Ping Kali

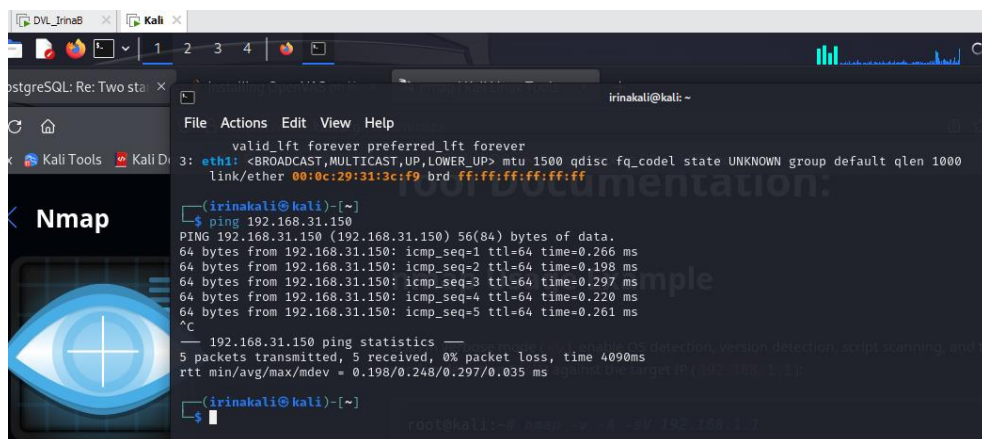


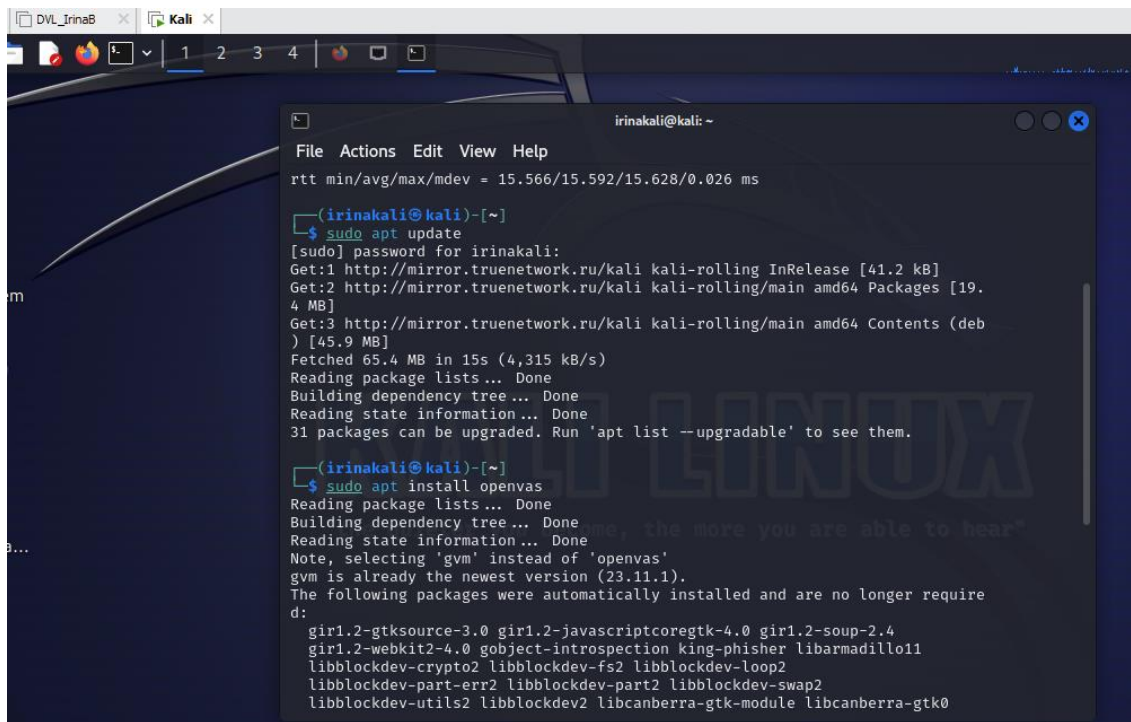
Рисунок 19 – Ping DVL

2 Анализ защищённости

2.1 Сканирование сети и уязвимостей

Шаг 3. Инструмент OpenVas

Установим OpenVas на уже имеющуюся VM Kali Linux (рис. 20).



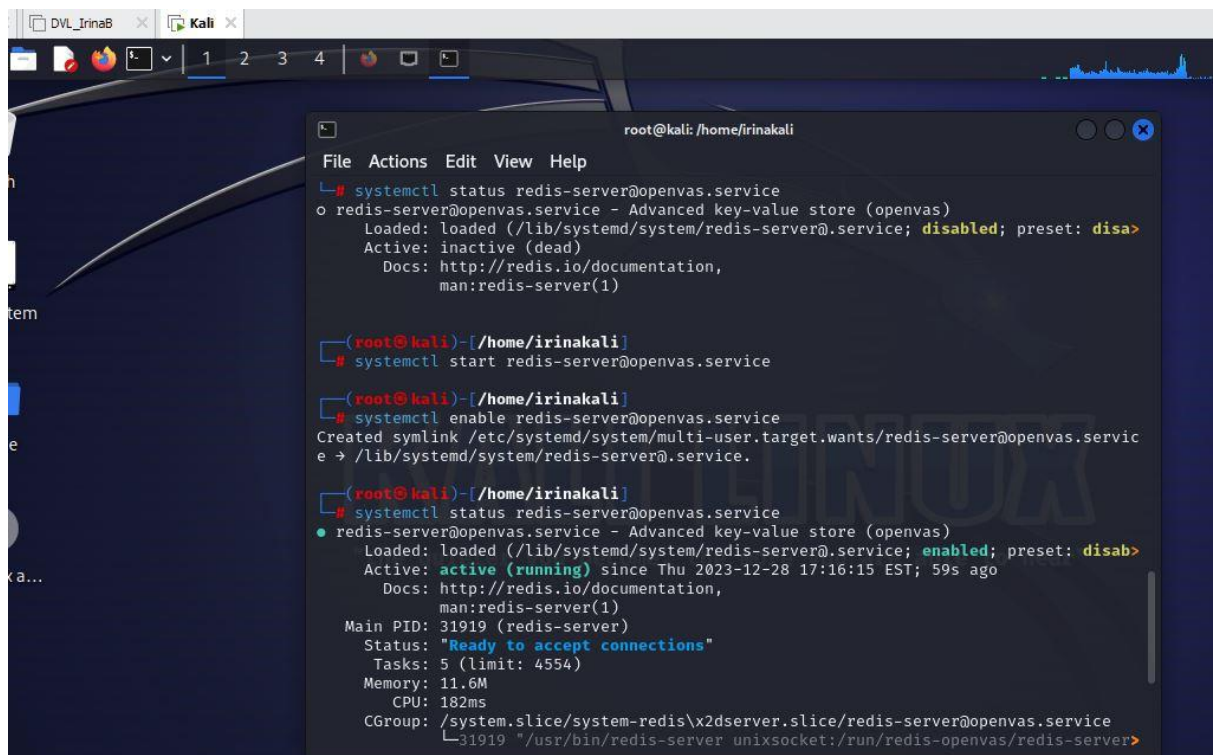
```
File Actions Edit View Help
rtt min/avg/max/mdev = 15.566/15.592/15.628/0.026 ms

(irinakali@kali)~$ sudo apt update
[sudo] password for irinakali:
Get:1 http://mirror.truenetwork.ru/kali kali-rolling InRelease [41.2 kB]
Get:2 http://mirror.truenetwork.ru/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://mirror.truenetwork.ru/kali kali-rolling/main amd64 Contents (deb) [45.9 MB]
Fetched 65.4 MB in 15s (4,315 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
31 packages can be upgraded. Run 'apt list --upgradable' to see them.

(irinakali@kali)~$ sudo apt install openvas
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'gvm' instead of 'openvas'
gvm is already the newest version (23.11.1).
The following packages were automatically installed and are no longer required:
  gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4
  gir1.2-webkit2-4.0 gobject-introspection king-phisher libarmadillo11
  libblockdev-crypto2 libblockdev-fs2 libblockdev-loop2
  libblockdev-part-err2 libblockdev-part2 libblockdev-swap2
  libblockdev-utils2 libblockdev2 libcanberra-gtk-module libcanberra-gtk0
```

Рисунок 20 – Установка OpenVas

OpenVAS поставляется с собственной службой Redis для Kali GNU/Linux. Убедимся, что сервис Redis настроен для корректной работы с OpenVAS командой «systemctl status redisserver@openvas.service» (рис. 21).



```
File Actions Edit View Help
root@kali: /home/irinakali

# systemctl status redis-server@openvas.service
o redis-server@openvas.service - Advanced key-value store (openvas)
  Loaded: loaded (/lib/systemd/system/redis-server@.service; disabled; preset: disa>
  Active: inactive (dead)
  Docs: http://redis.io/documentation,
        man:redis-server(1)

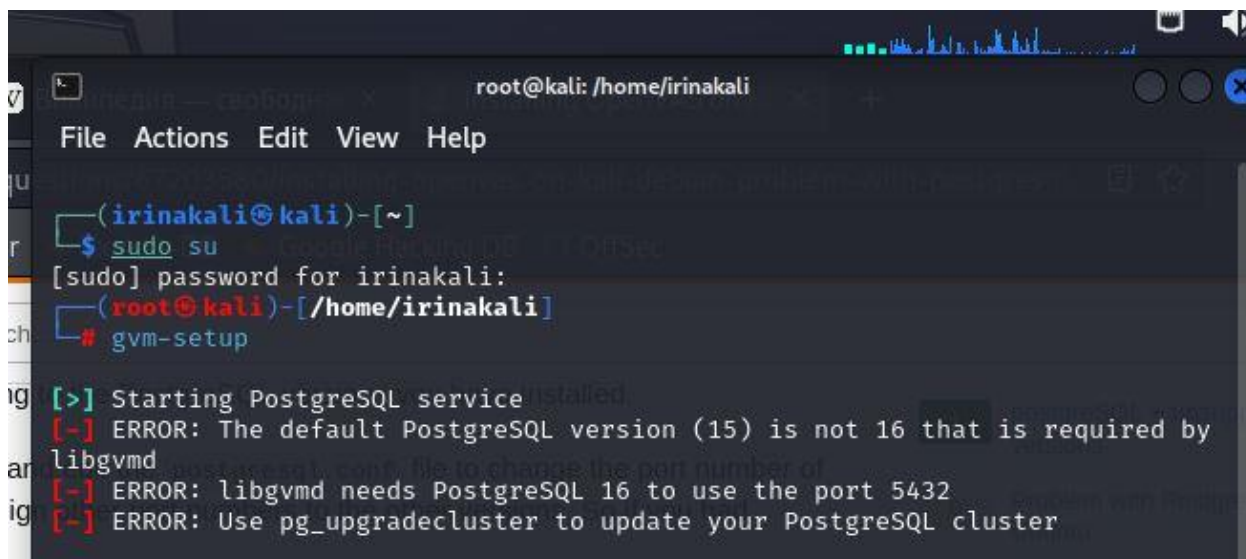
(root@kali)~[/home/irinakali]# systemctl start redis-server@openvas.service

(root@kali)~[/home/irinakali]# systemctl enable redis-server@openvas.service
Created symlink /etc/systemd/system/multi-user.target.wants/redis-server@openvas.servic
e -> /lib/systemd/system/redis-server@.service.

(root@kali)~[/home/irinakali]# systemctl status redis-server@openvas.service
● redis-server@openvas.service - Advanced key-value store (openvas)
  Loaded: loaded (/lib/systemd/system/redis-server@.service; enabled; preset: disab>
  Active: active (running) since Thu 2023-12-28 17:16:15 EST; 59s ago
  Docs: http://redis.io/documentation,
        man:redis-server(1)
  Main PID: 31919 (redis-server)
  Status: "Ready to accept connections"
  Tasks: 5 (limit: 4554)
  Memory: 11.6M
  CPU: 182ms
  CGroup: /system.slice/system-redis\x2dserver.slice/redis-server@openvas.service
          └─31919 /usr/bin/redis-server unixsocket:/run/redis-openvas/redis-server>
```

Рисунок 21 – Статус Redis

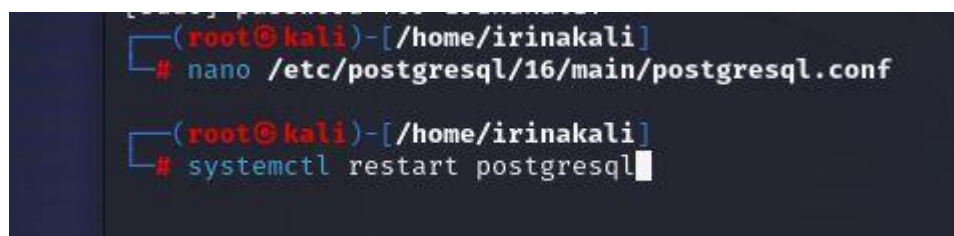
При попытке запустить настройку сервиса, получаем ошибку о версии СУБД (рис. 22).



```
root@kali: /home/irinakali
File Actions Edit View Help
(irinakali@kali)-[~]
$ sudo su
[sudo] password for irinakali:
(root@kali)-[/home/irinakali]
# gvm-setup
[>] Starting PostgreSQL service installed
[-] ERROR: The default PostgreSQL version (15) is not 16 that is required by libgvmd
[-] ERROR: libgvmd needs PostgreSQL 16 to use the port 5432
[-] ERROR: Use pg_upgradecluster to update your PostgreSQL cluster
```

Рисунок 22 – Ошибка версии

Для решения данной проблемы необходимо заменить порт необходимой версии на 5432 (рис. 24). Не забудем перезапустить сервис СУБД командой «sudo systemctl restart postgresql» (рис. 23).



```
(root@kali)-[/home/irinakali]
# nano /etc/postgresql/16/main/postgresql.conf

(root@kali)-[/home/irinakali]
# systemctl restart postgresql
```

Рисунок 23 – Перезапуск

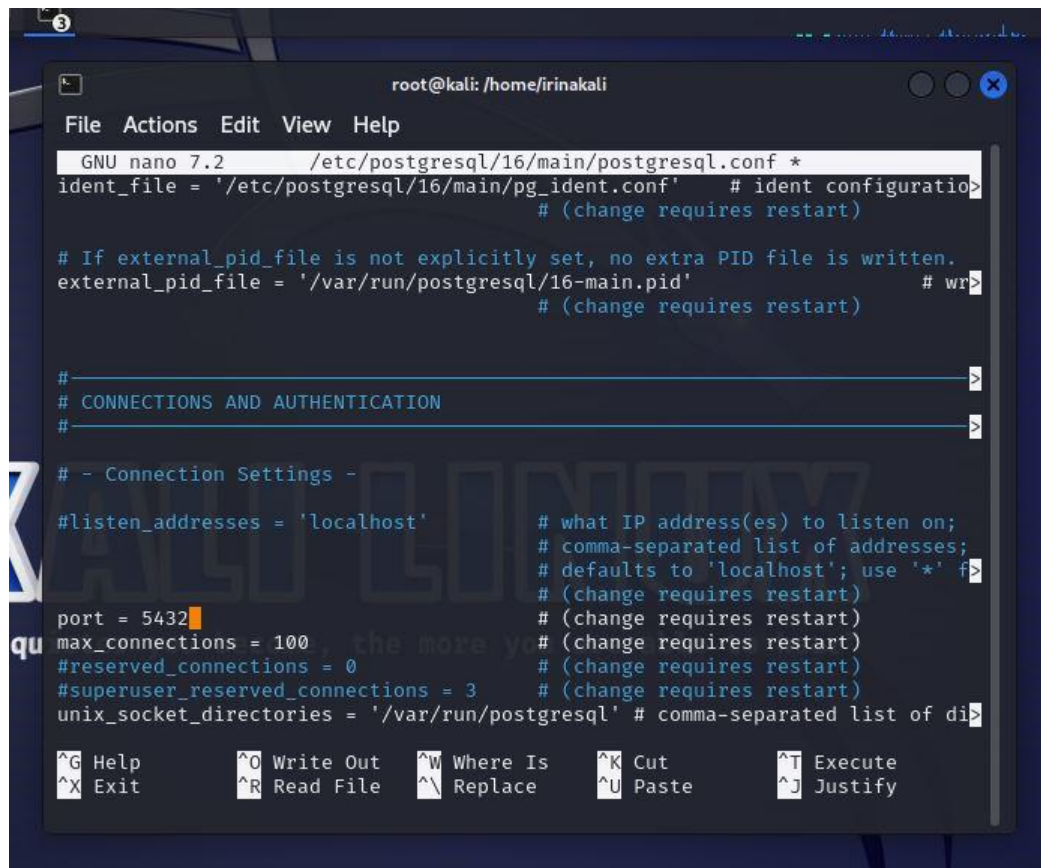


Рисунок 24 – Замена порта СУБД

Но возникла новая проблема, версии не совпадали (рис. 25).

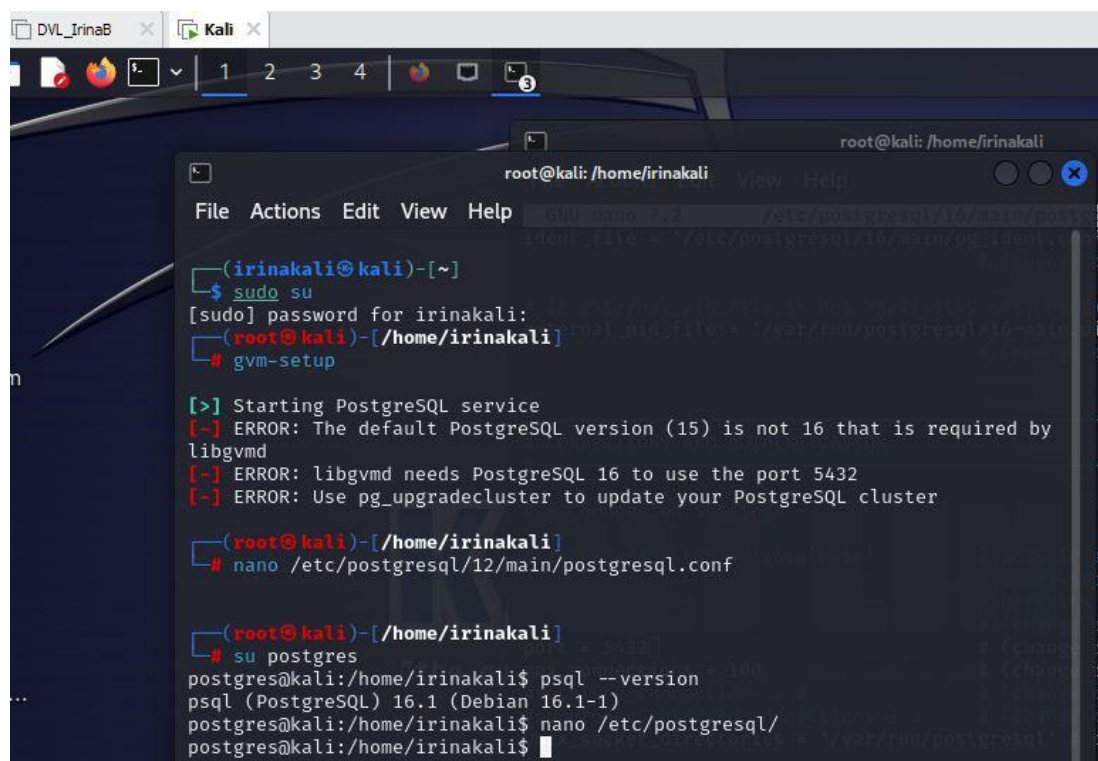
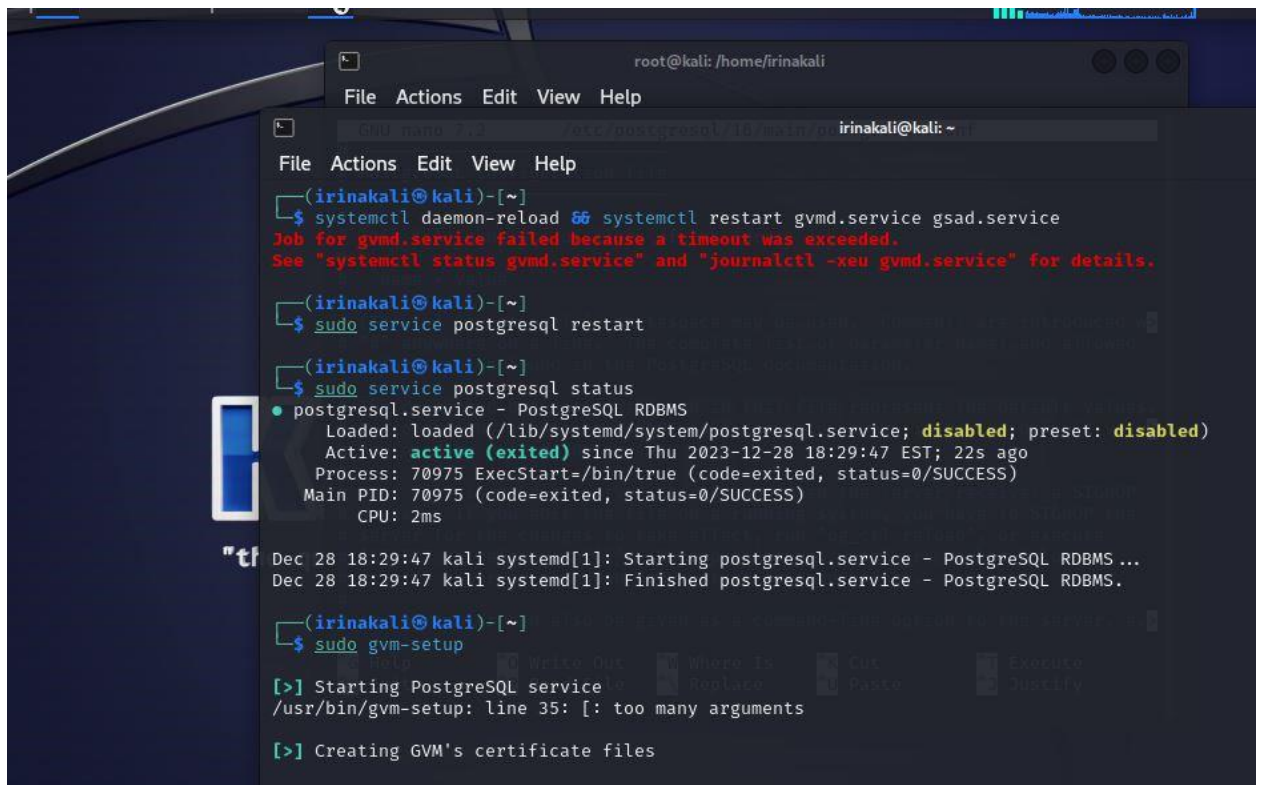


Рисунок 25 – Очередная ошибка



```
root@kali: /home/irinakali
File Actions Edit View Help

GNU nano 2.9.3 /etc/postgresql/16/main/postgresql.conf
irinakali@kali: ~
File Actions Edit View Help

(irinakali@kali)~$ systemctl daemon-reload
Job for gvm.service failed because a timeout was exceeded.
See "systemctl status gvm.service" and "journalctl -xeu gvm.service" for details.

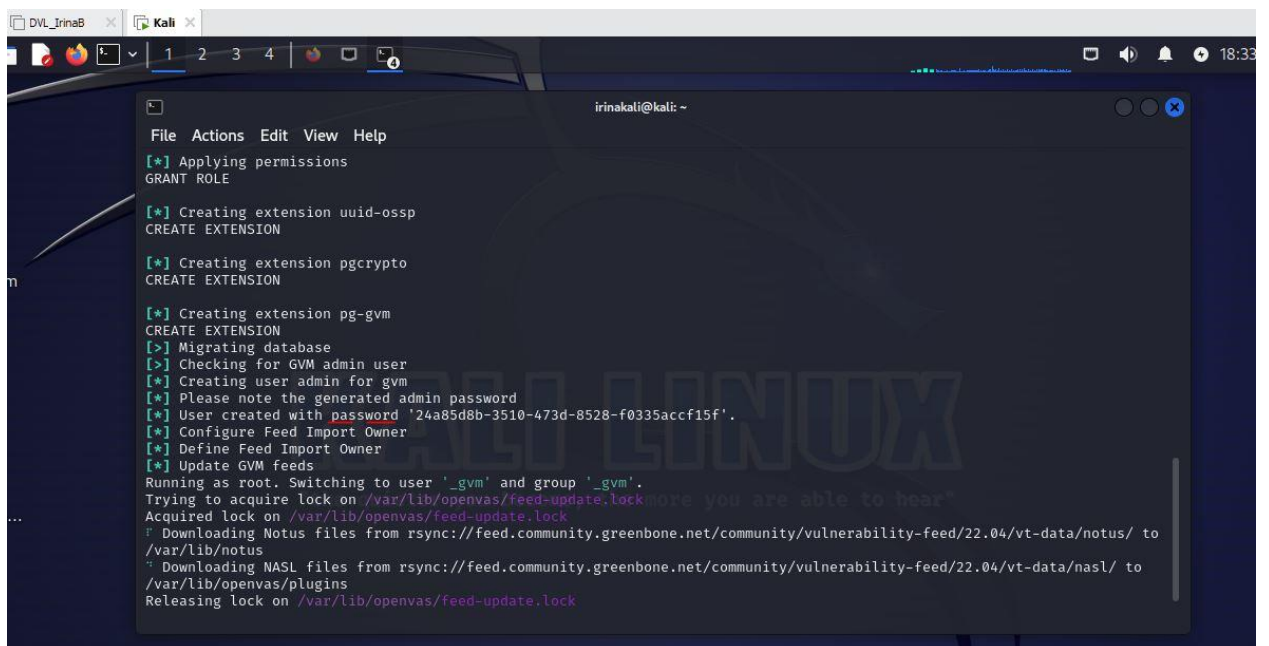
(irinakali@kali)~$ sudo service postgresql restart
postgresql.service - PostgreSQL RDBMS
Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
Active: active (exited) since Thu 2023-12-28 18:29:47 EST; 22s ago
Process: 70975 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
Main PID: 70975 (code=exited, status=0/SUCCESS)
CPU: 2ms

Dec 28 18:29:47 kali systemd[1]: Starting postgresql.service - PostgreSQL RDBMS ...
Dec 28 18:29:47 kali systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

(irinakali@kali)~$ sudo gvm-setup
[>] Starting PostgreSQL service
/usr/bin/gvm-setup: line 35: [: too many arguments

[>] Creating GVM's certificate files
```

Рисунок 28 – Запуск



```
irinakali@kali: ~
File Actions Edit View Help

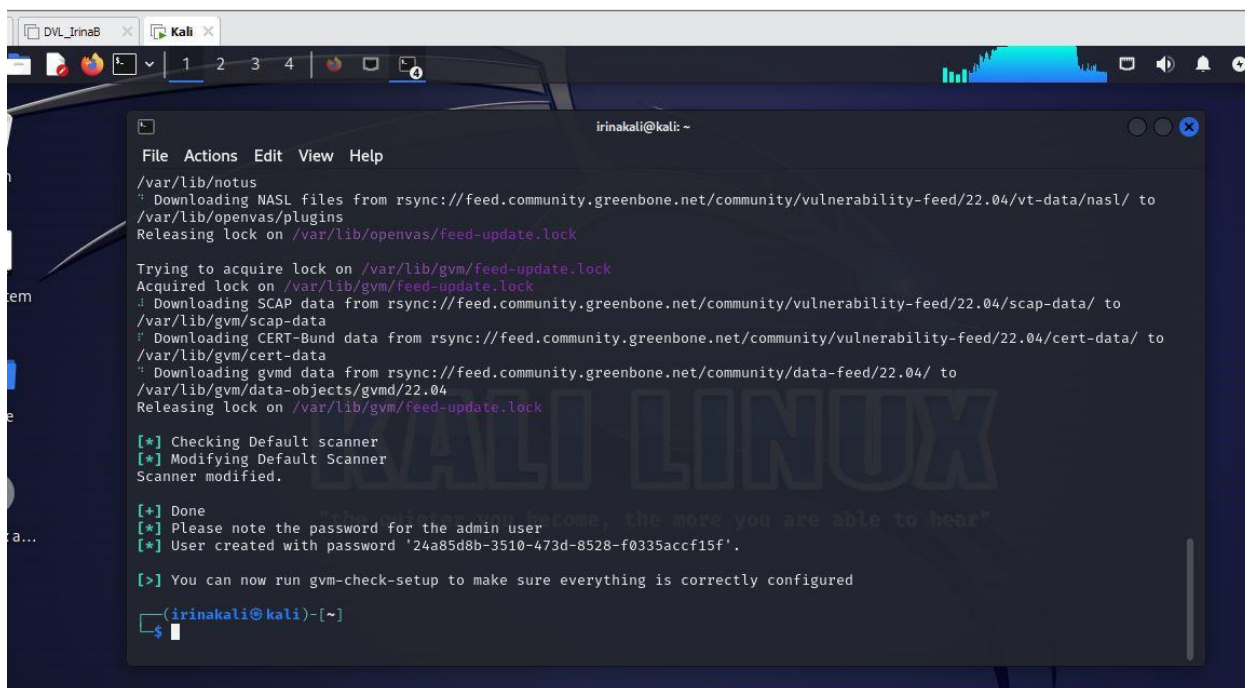
[*] Applying permissions
GRANT ROLE

[*] Creating extension uuid-ossp
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 '24a85d8b-3510-473d-8528-f0335accf15f'.
[*] 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
```

Рисунок 29 – Первичная настройка сервиса



```
File Actions Edit View Help
/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 gvmdata 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

[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.

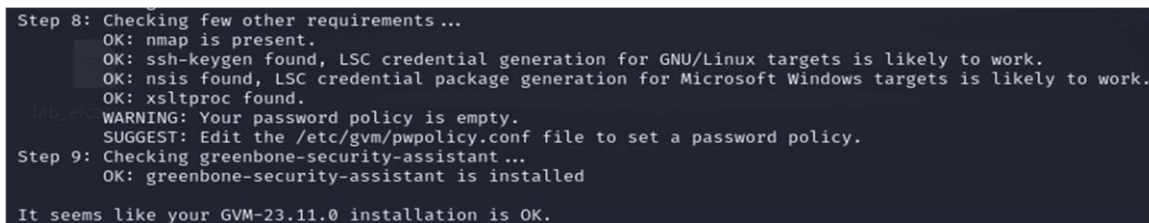
[+] Done
[*] Please note the password for the admin user: 'come, the more you are able to hear'
[*] User created with password '24a85d8b-3510-473d-8528-f0335accf15f'.

[>] You can now run gvm-check-setup to make sure everything is correctly configured

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

Рисунок 30 – Результат

Дождемся конца установки. По окончании настройки проверим успешность установки командой «`sudo gvm-check-setup`», но у нас возникает ошибка (рис. 31).



```
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: nsis found, LSC credential package generation for Microsoft Windows targets is likely to work.
OK: xsftproc 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.
```

Рисунок 31– Проверка установки

Настройка OpenVAS.

Настроим сервис `gvmd` и обновим базу OpenVAS, включим сервис `gvmd` (рис. 32).



```
$ 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
```

Рисунок 32 – Обновление базы

Переходим в веб-интерфейс по адресу <https://localhost:9392/>. Вводим учетные данные пользователя и сразу попадаем на главную страницу (рис. 33-34).

Данные для входа:

Please note the generated admin password

[*] User created with password '24a85d8b-3510-473d-8528-f0335accf15f '.

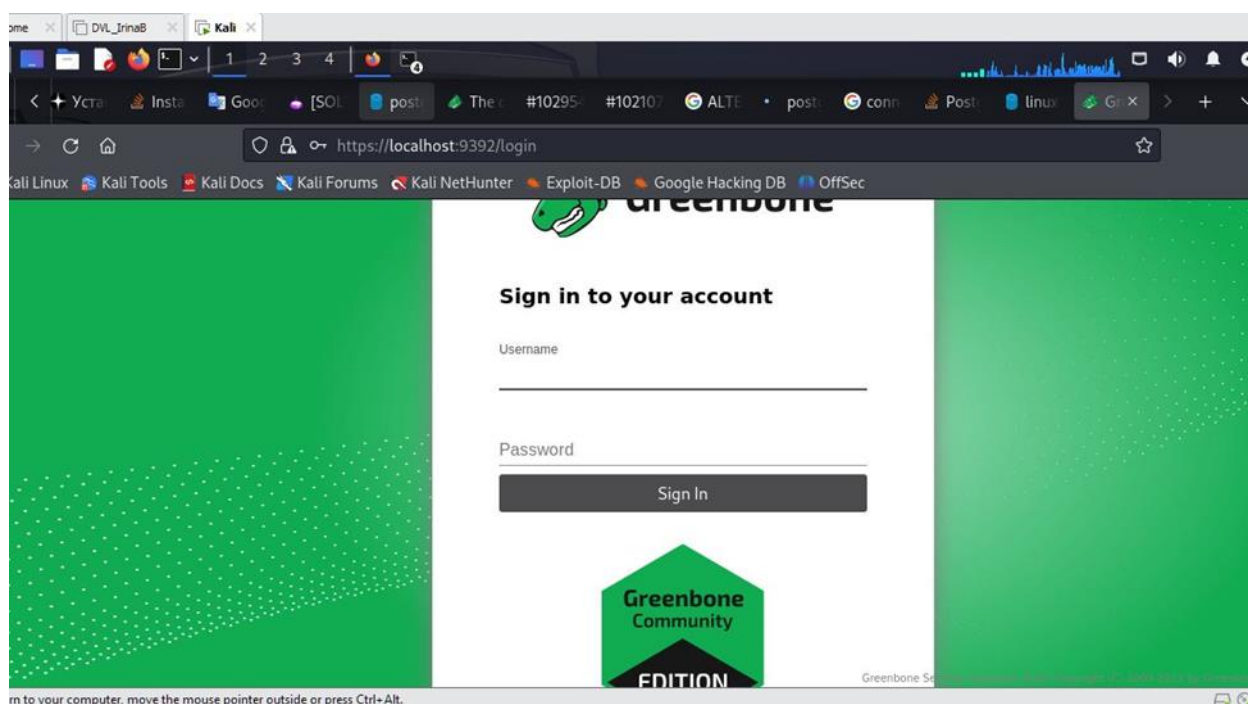


Рисунок 33 – Ввод учётной записи OpenVAS

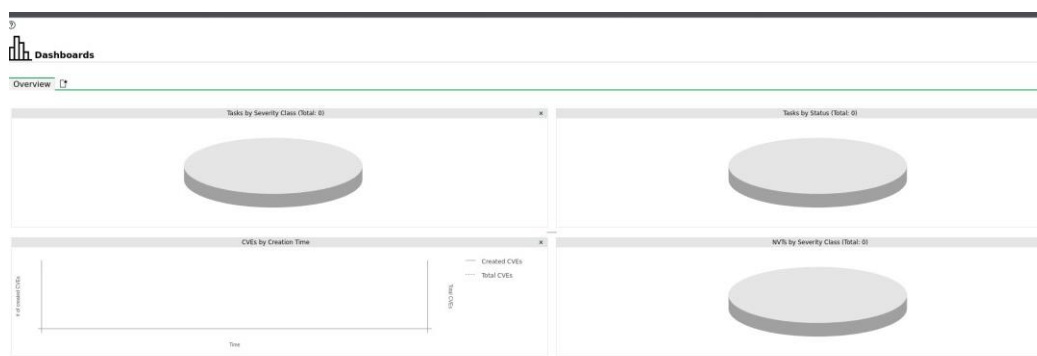


Рисунок 34 – Главная страница веб-интерфейса OpenVAS

Сканирование сети с помощью OpenVAS.

Проведем операции по сканированию сети. Создадим задачу на сканирование нашего целевого узла (рисунок 35).

Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname:

The default address is either your computer or your network gateway.
As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon you can create a new Task yourself.

Cancel

Start Scan

Рисунок 35 – Создание задачи

Теперь посмотрим, что находится в отчете по итогам сканирования узла (рисунки 36-37).

Information	Results (2 of 17)	Hosts (1 of 1)	Ports (0 of 2)	Applications (4 of 4)	Operating Systems (1 of 1)
Application CPE					
cpe:/a:apple:cups:1.1					
cpe:/a:openprinting:cups:1.1					
cpe:/a:mysql:mysql					

Рисунок 36 – Обнаруженные приложения на узле

Information	Results (2 of 17)	Hosts (1 of 1)	Ports (0 of 2)	Applications (4 of 4)	Operating Systems (1 of 1)	CVEs (1 of 1)	Closed CVEs (0 of 0)	TLS Certificates (0 of 0)	Error Messages (0 of 0)	User Tags (0)
CVE						NVT				
CVE-1999-0524						ICMP Timestamp Reply Information Disclosure				

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Рисунок 37 – Обнаруженные CVE на узле

Если нажать на уязвимость, то будет отображено её подробное описание.

Запущен сервис ssh на DVL (рис. 38):

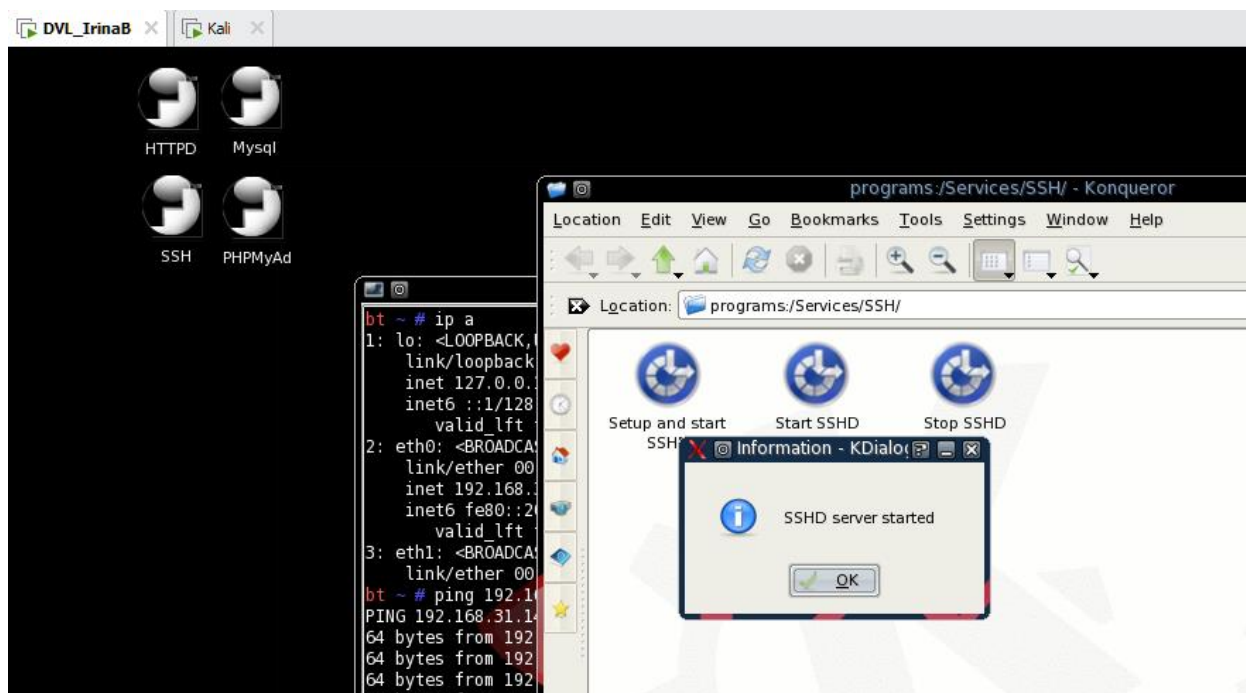


Рисунок 38 – ssh на DVL

Шаг 4. Инструмент Nmap

Проведем операции по сканированию сети. Выполним поиск узлов в подсети (рис. 39).

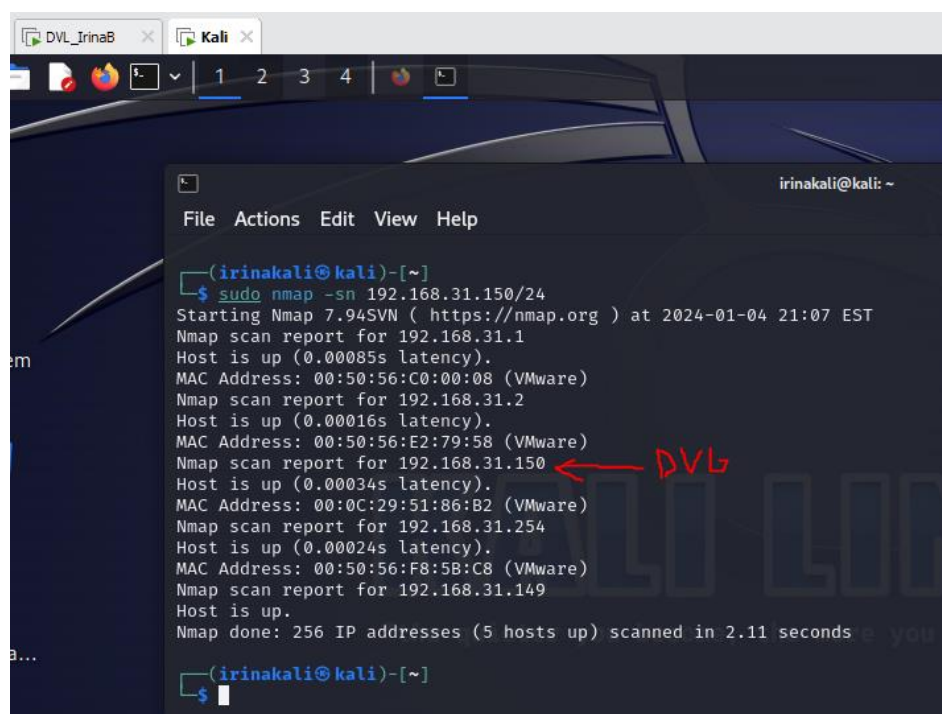
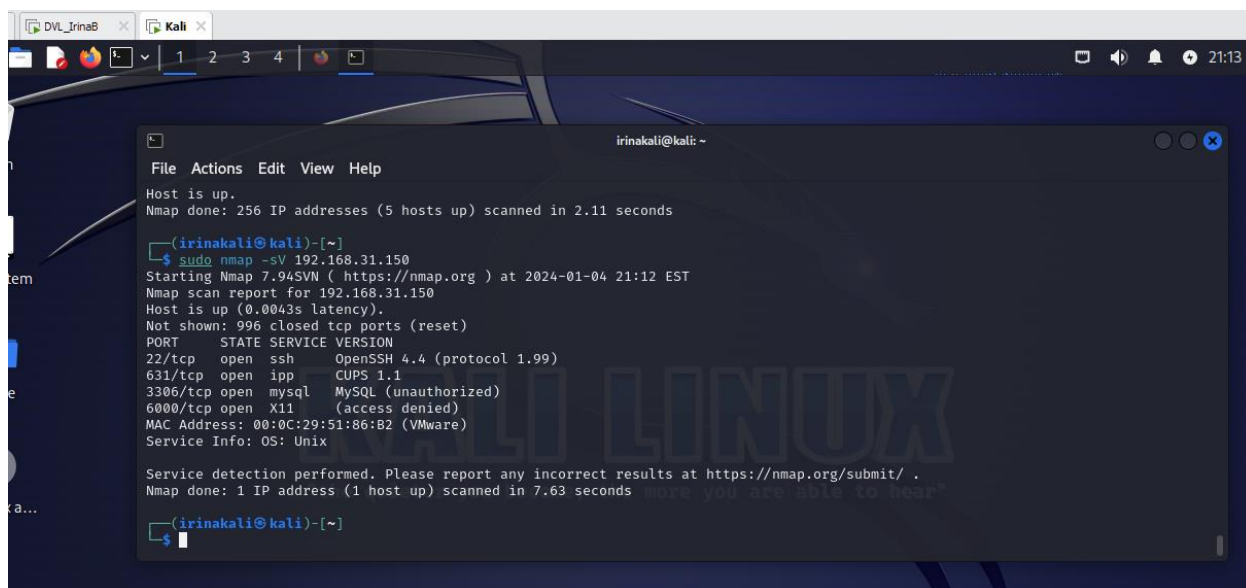


Рисунок 39 – Поиск узлов

Затем просканируем конкретный узел с целью выявления рабочих сервисов и портов, по которым они выходят наружу (рис. 40).



```
File Actions Edit View Help
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.11 seconds

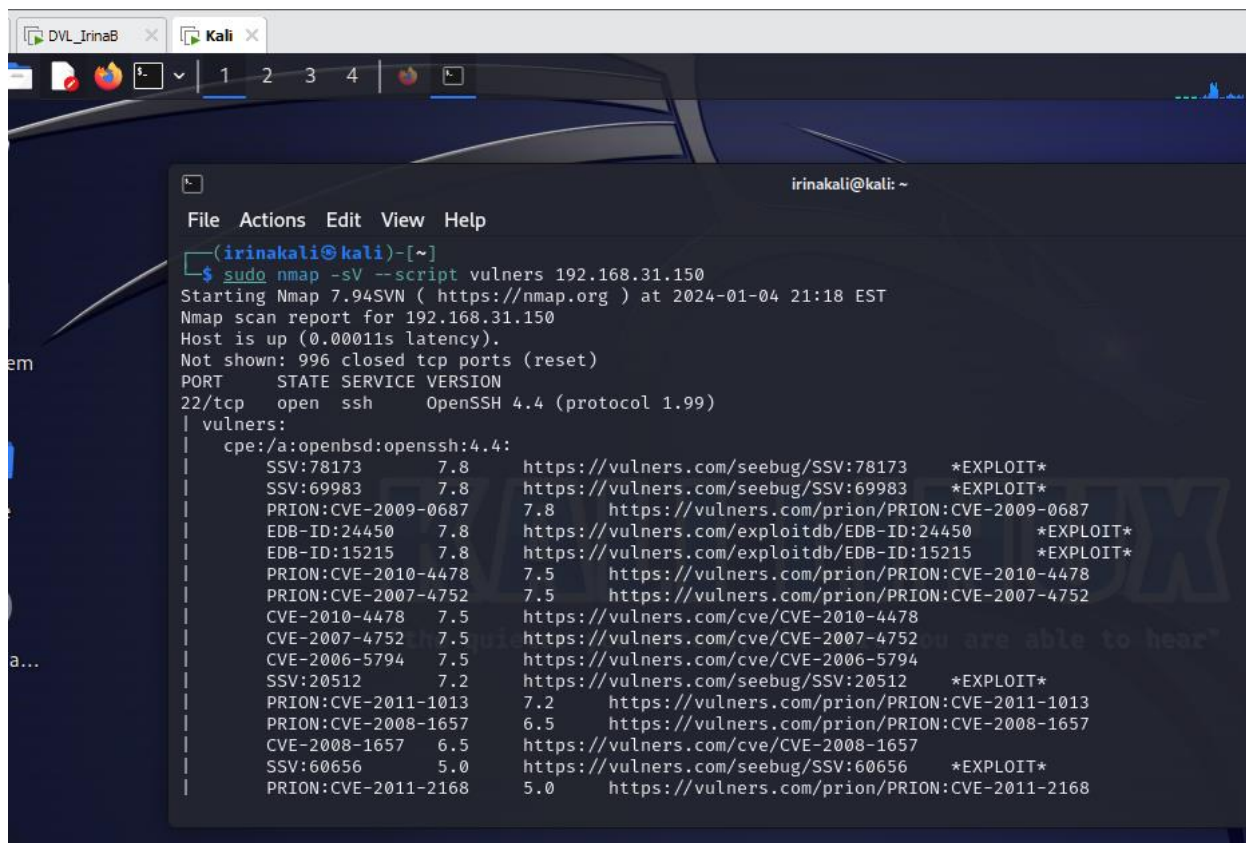
(irinakali@kali)-[~]
$ sudo nmap -sV 192.168.31.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 21:12 EST
Nmap scan report for 192.168.31.150
Host is up (0.0043s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.4 (protocol 1.99)
631/tcp    open  ipp      CUPS 1.1
3306/tcp   open  mysql    MySQL (unauthorized)
6000/tcp   open  X11      (access denied)
MAC Address: 00:0C:29:51:86:B2 (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.63 seconds

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

Рисунок 40 – Запрос по сервисам

После чего попробуем просканировать узел на наличие потенциальных угроз безопасности (рис. 41).



```
File Actions Edit View Help
(irinakali@kali)-[~]
$ sudo nmap -sV --script vulners 192.168.31.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 21:18 EST
Nmap scan report for 192.168.31.150
Host is up (0.00011s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.4 (protocol 1.99)
| vulners:
| cpe:/a:openbsd:openssh:4.4:
| SSV:78173      7.8 https://vulners.com/seebug/SSV:78173 *EXPLOIT*
| SSV:69983      7.8 https://vulners.com/seebug/SSV:69983 *EXPLOIT*
| PRION:CVE-2009-0687 7.8 https://vulners.com/prion/PRION:CVE-2009-0687
| EDB-ID:24450    7.8 https://vulners.com/exploitdb/EDB-ID:24450 *EXPLOIT*
| EDB-ID:15215    7.8 https://vulners.com/exploitdb/EDB-ID:15215 *EXPLOIT*
| PRION:CVE-2010-4478 7.5 https://vulners.com/prion/PRION:CVE-2010-4478
| PRION:CVE-2007-4752 7.5 https://vulners.com/prion/PRION:CVE-2007-4752
| CVE-2010-4478    7.5 https://vulners.com/cve/CVE-2010-4478
| 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-2011-1013 7.2 https://vulners.com/prion/PRION:CVE-2011-1013
| 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:60656      5.0 https://vulners.com/seebug/SSV:60656 *EXPLOIT*
| PRION:CVE-2011-2168 5.0 https://vulners.com/prion/PRION:CVE-2011-2168
```

```
File Actions Edit View Help
PRION:CVE-2011-1013 7.2 https://vulners.com/prion/PRION:CVE-2011-1013
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:60656 5.0 https://vulners.com/seebug/SSV:60656 *EXPLOIT*
PRION:CVE-2011-2168 5.0 https://vulners.com/prion/PRION:CVE-2011-2168
PRION:CVE-2010-5107 5.0 https://vulners.com/prion/PRION:CVE-2010-5107
PRION:CVE-2009-0780 5.0 https://vulners.com/prion/PRION:CVE-2009-0780
PRION:CVE-2008-4109 5.0 https://vulners.com/prion/PRION:CVE-2008-4109
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-2010-5107 5.0 https://vulners.com/cve/CVE-2010-5107
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:B5E7D30E7583980F37EF6DBC0B05FBC3 4.9 https://vulners.com/exploitpack/EXPLOITPACK:B5E7D30E7583980F37EF6DBC0B05FBC3 *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-2010-4755 4.0 https://vulners.com/prion/PRION:CVE-2010-4755
PRION:CVE-2012-0814 3.5 https://vulners.com/prion/PRION:CVE-2012-0814
PRION:CVE-2011-5000 3.5 https://vulners.com/prion/PRION:CVE-2011-5000
CVE-2012-0814 3.5 https://vulners.com/cve/CVE-2012-0814
CVE-2011-5000 3.5 https://vulners.com/cve/CVE-2011-5000
```

```
File Actions Edit View Help
|_ SECURITYVULNS:VULN:9830 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:9830
631/tcp open ipp CUPS 1.1
|_ http-server-header: CUPS/1.1
vulners:
|_ cpe:/a:apple:cups:1.1:
|_ SSV:3063 10.0 https://vulners.com/seebug/SSV:3063 *EXPLOIT*
|_ SSV:2375 10.0 https://vulners.com/seebug/SSV:2375 *EXPLOIT*
|_ SECURITYVULNS:VULN:8724 10.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:8724
|_ PRION:CVE-2008-5184 10.0 https://vulners.com/prion/PRION:CVE-2008-5184
|_ PRION:CVE-2008-3641 10.0 https://vulners.com/prion/PRION:CVE-2008-3641
|_ PRION:CVE-2008-0053 10.0 https://vulners.com/prion/PRION:CVE-2008-0053
|_ PRION:CVE-2007-4351 10.0 https://vulners.com/prion/PRION:CVE-2007-4351
|_ CVE-2008-5184 10.0 https://vulners.com/cve/CVE-2008-5184
|_ CVE-2008-3641 10.0 https://vulners.com/cve/CVE-2008-3641
|_ CVE-2008-0053 10.0 https://vulners.com/cve/CVE-2008-0053
|_ CVE-2007-4351 10.0 https://vulners.com/cve/CVE-2007-4351
|_ SSV:2771 9.4 https://vulners.com/seebug/SSV:2771 *EXPLOIT*
|_ SSV:3058 9.3 https://vulners.com/seebug/SSV:3058 *EXPLOIT*
|_ SECURITYVULNS:VULN:10333 9.3 https://vulners.com/securityvulns/SECURITYVULNS:VULN:10333
|_ PRION:CVE-2010-2941 7.9 https://vulners.com/prion/PRION:CVE-2010-2941
|_ CVE-2010-2941 7.9 https://vulners.com/cve/CVE-2010-2941
|_ SSV:5067 7.5 https://vulners.com/seebug/SSV:5067 *EXPLOIT*
|_ PRION:CVE-2010-3702 7.5 https://vulners.com/prion/PRION:CVE-2010-3702
|_ PRION:CVE-2009-1182 7.5 https://vulners.com/prion/PRION:CVE-2009-1182
|_ PRION:CVE-2008-3639 7.5 https://vulners.com/prion/PRION:CVE-2008-3639
|_ CVE-2010-3702 7.5 https://vulners.com/cve/CVE-2010-3702
```

```
DVL_IrinaB x Kali x
File Actions Edit View Help
CVE-2010-2431 2.6 https://vulners.com/cve/CVE-2010-2431
PRION:CVE-2014-5030 1.9 https://vulners.com/prion/PRION:CVE-2014-5030
CVE-2014-5030 1.9 https://vulners.com/cve/CVE-2014-5030
PRION:CVE-2021-25317 1.7 https://vulners.com/prion/PRION:CVE-2021-25317
PRION:CVE-2014-3537 1.2 https://vulners.com/prion/PRION:CVE-2014-3537
PRION:CVE-2013-6891 1.2 https://vulners.com/prion/PRION:CVE-2013-6891
CVE-2014-3537 1.2 https://vulners.com/cve/CVE-2014-3537
CVE-2013-6891 1.2 https://vulners.com/cve/CVE-2013-6891
SECURITYVULNS:VULN:5184 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:5184
SECURITYVULNS:VULN:4277 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:4277
SECURITYVULNS:VULN:4109 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:4109
SECURITYVULNS:VULN:4010 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:4010
SECURITYVULNS:VULN:293 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:293
SECURITYVULNS:VULN:2888 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:2888
SECURITYVULNS:VULN:2490 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:2490
3306/tcp open mysql MySQL (unauthorized)
6000/tcp open X11 (access denied)
MAC Address: 00:0C:29:51:86:B2 (VMware)
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.57 seconds
(irinakali@kali)-[~]
```

Рисунок 41 – Поиск уязвимостей

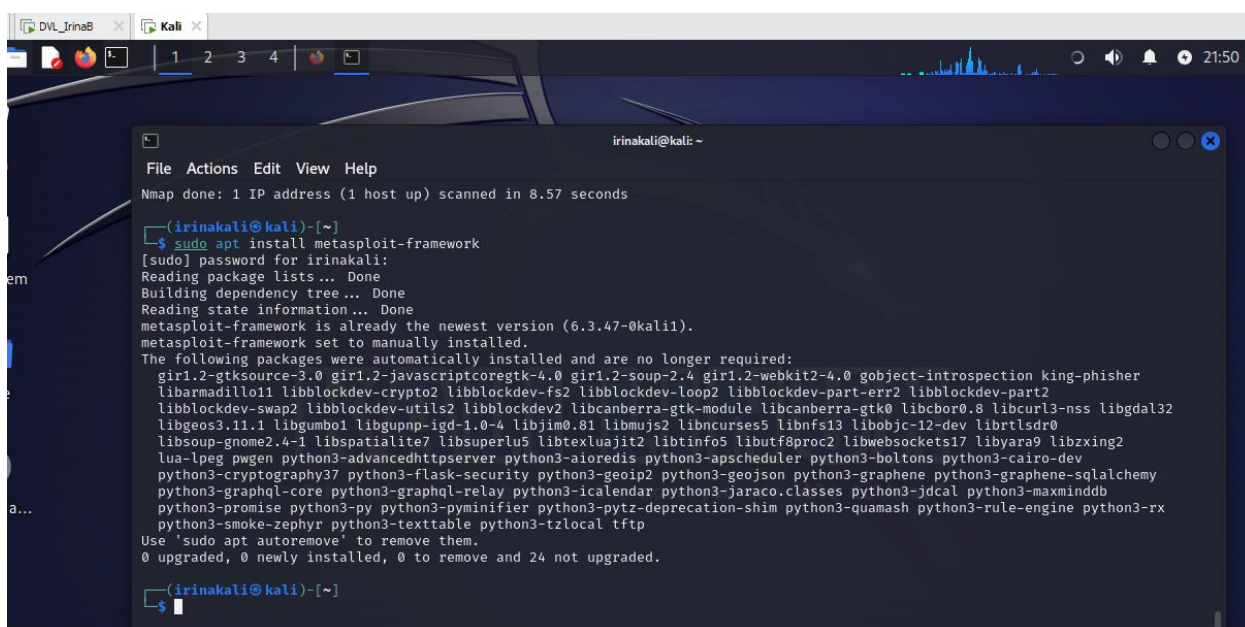
В сравнении с nmap, OpenVAS нашел гораздо меньше уязвимостей, что связано, в первую очередь, с базовым скриптом и базовой базой уязвимостей, которые участвуют в сканировании.

Преимуществом OpenVAS будет являться функционал по визуализации и настройке расписания сканирований, что будет полезным при постоянном мониторинге узлов в сети на предмет возможных уязвимостей.

3 Анализ безопасности системы

3.1 Инструмент Metasploit

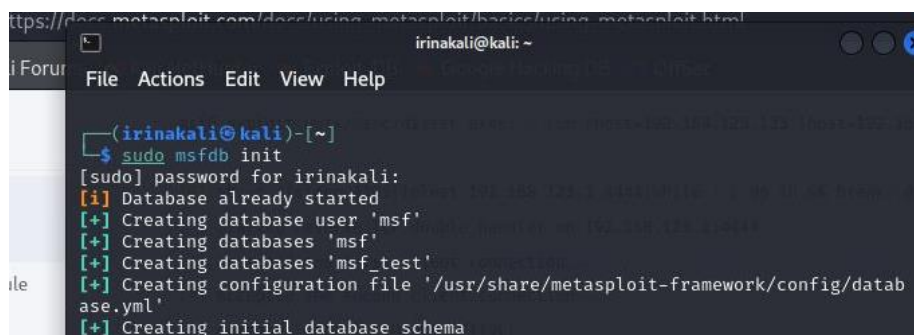
Установка Metasploit, обновление и запуск (рис. 42-44).



```
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 8.57 seconds

(irinakali@kali)-[~]
└─$ sudo apt install metasploit-framework
[sudo] password for irinakali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
metasploit-framework is already the newest version (6.3.47-0kali1).
metasploit-framework set to manually installed.
The following packages were automatically installed and are no longer required:
  gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gir1.2-webkit2-4.0 gobject-introspection king-phisher
  libarmadillo11 libblockdev-crypto2 libblockdev-fs2 libblockdev-loop2 libblockdev-part-err2 libblockdev-part2
  libblockdev-swap2 libblockdev-utils2 libblockdev2 libcanberra-gtk-module libcanberra-gtk0 libchor0.8 libcurl3-nss libgdal32
  libgeos3.11.1 libgumbo1 libgupnp-igd-1.0-4 libjim0.81 libmuj2 libncurses5 libnfs13 libobjc-12-dev librtlsdr0
  libsoup-gnome2.4-1 libspatialite7 libsuperlu5 libtexluajit2 libtinfo5 libutf8proc2 libwebsockets17 libyara9 libzxing2
  lua-lpeg pwgen python3-advancedhttpserver python3-aioredis python3-apscheduler python3-bolttons python3-cairo-dev
  python3-cryptography37 python3-flask-security python3-geoip2 python3-geojson python3-graphene python3-graphene-sqlalchemy
  python3-graphql-core python3-graphql-relay python3-icalendar python3-jaraco.classes python3-jdcal python3-maxminddb
  python3-promise python3-py python3-pyminifier python3-pytz-deprecation-shim python3-quamash python3-rule-engine python3-rx
  python3-smoke-zephyr python3-texttable python3-tzlocal tftp
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 24 not upgraded.
```

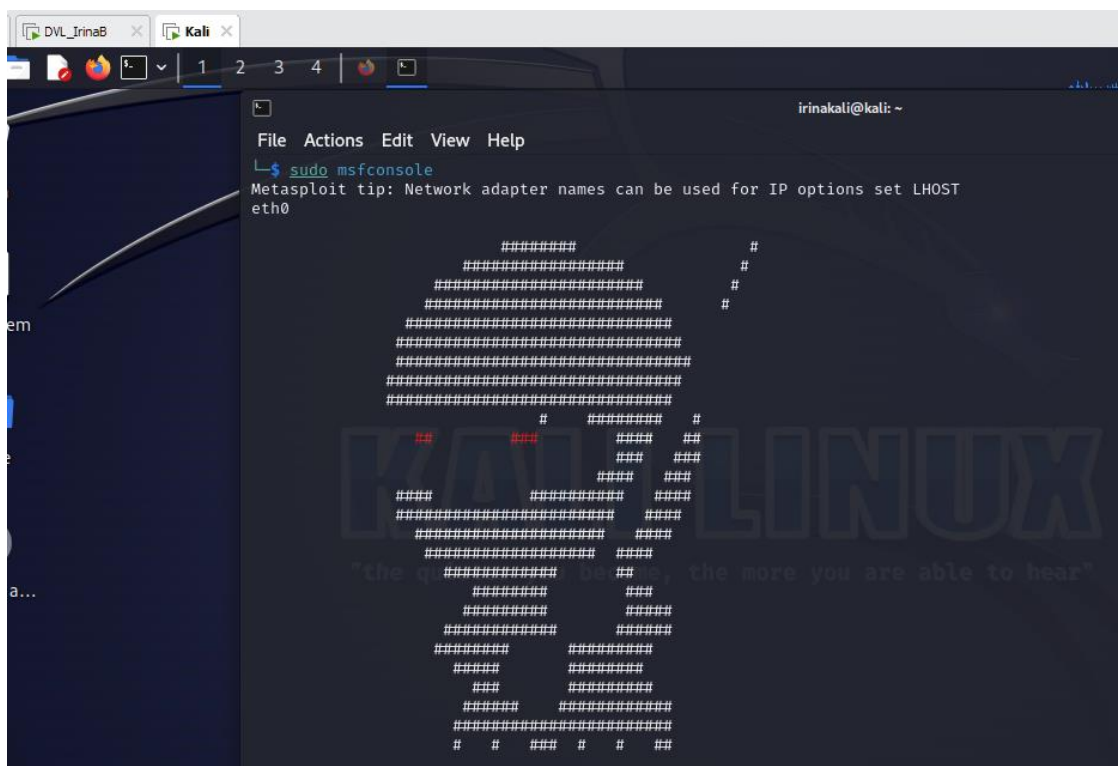
Рисунок 42 – Установка Metasploit



```
File Actions Edit View Help

(irinakali@kali)-[~]
└─$ sudo msfdb init
[sudo] password for irinakali:
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

Рисунок 43 – Обновление и запуск



Посмотрим какие функциональные возможности нам предлагает утилита в отношении SSH (рис. 45).

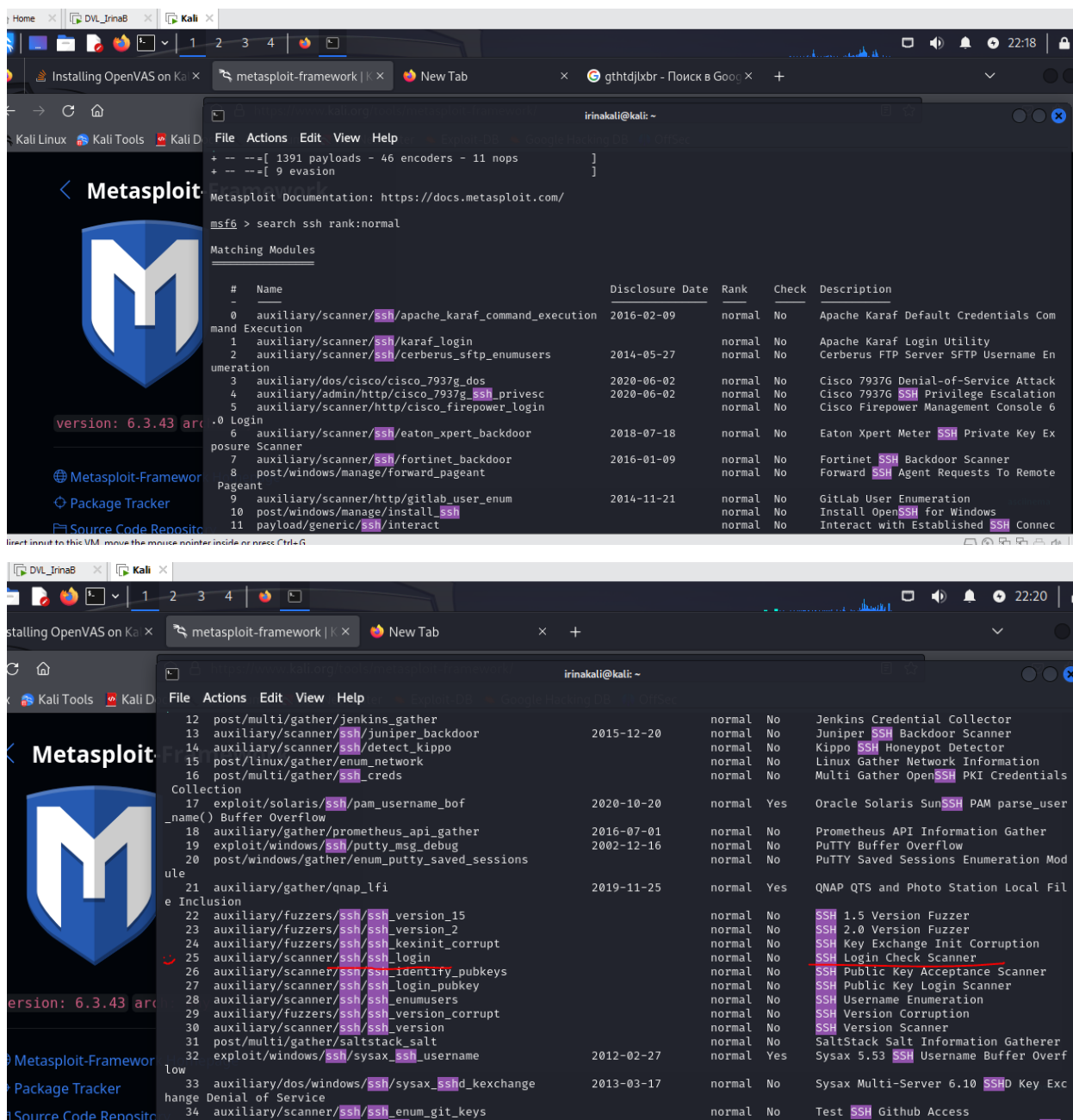


Рисунок 45 – Поиск вектора

Выберем вариант – сканер логина под номером «25», пропишем «use 25». Из представленных функцией опций нам потребуется только указание целевого узла и подключение словаря в формате «логин пароль». Укажем необходимые опции и запустим (рис. 46).

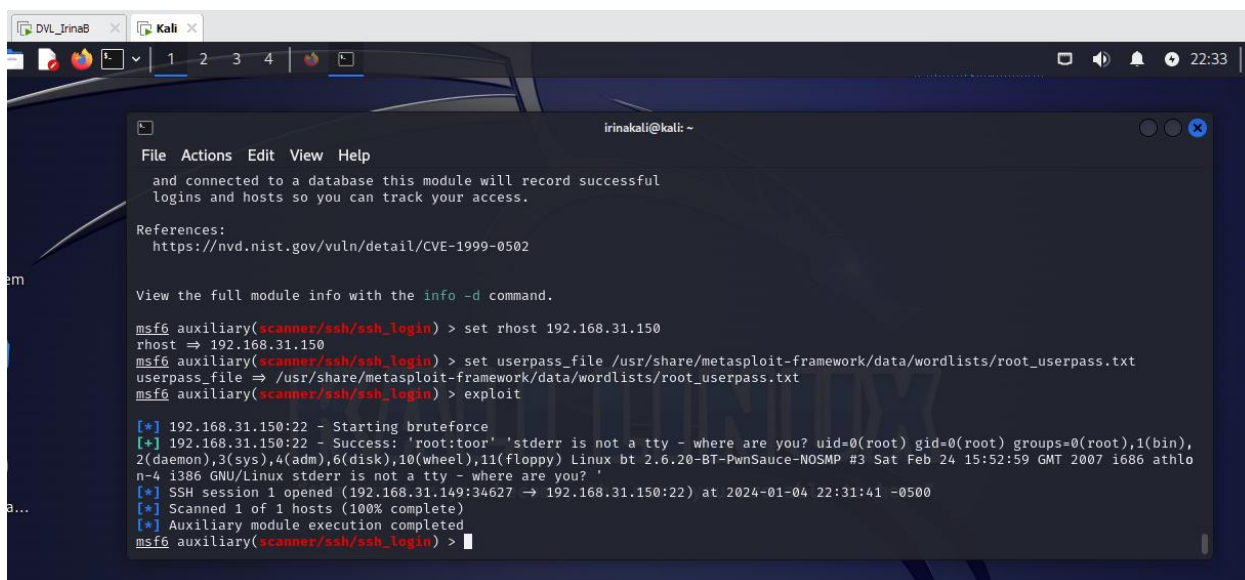


Рисунок 46 – Подготовка и запуск

Было получено совпадение с кредами целевого узла для подключения по SSH. Данная уязвимость имеет идентификатор «CVE-1999-0502» и подразумевает, что для сервиса SSH установлена учетная запись Unix, которая имеет пароль по умолчанию, нулевой, пустой или отсутствующий. CVE-1999-0502 относится к уязвимости в протоколе управления передачей (TCP) стека протоколов TCP/IP, которая также может привести к отказу в обслуживании (DoS). Уязвимость связана с возможностью переполнения буфера в функции `recv()` в коде BSD.

Рекомендации по устранению данной уязвимости:

1. Следует отключить учетную запись `root` или задать ей сложный пароль.
2. Использовать авторизацию по приватному ключу.
3. Использовать двухфакторную аутентификацию для SSH.
4. Убедиться, что на сервере и клиентских машинах установлены последние обновления безопасности для операционной системы и приложений.
5. Обновить программное обеспечение, использующее уязвимые функции, до последних версий, в которых уязвимость была исправлена.

6. Если это невозможно, отключить использование уязвимых функций или измените конфигурацию, чтобы избежать их использования. Например, если уязвимость связана с функцией `recv()`, можно попробовать использовать альтернативные функции для чтения данных.

7. Ограничить доступ к уязвимым функциям или службам, которые их используют, только для доверенных источников и пользователей.

8. Использовать системы предотвращения вторжений и брандмауэры для защиты от возможных атак, использующих уязвимость.

9. Постоянно следить за обновлениями безопасности и новыми угрозами, связанными с этой уязвимостью, и своевременно применять необходимые исправления.

Заключение

В ходе выполнения данной практической работы цель работы была достигнута и были выполнены следующие задачи:

Сканирование сети с помощью Nmap;

Сканирование сети с помощью OpenVAS;

Анализ безопасности системы с помощью Metasploit.