



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

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Практическая работа

по дисциплине

«Управление информационной безопасностью»

Группа:
ББМО-01-22
Выполнила:
Огольцова Н.Д.

Проверил:
Пимонов Р.В.

Москва 2023

Задание 1. Развёртывание и настройка.

Скачаем DVL образ диска.

Back About Release | Download | Description | File information | Virtual Machine | Networking | Screenshot(s) | Walkthrough(s)

DAMN VULNERABLE LINUX (DVL): 1.5 (INFECTIOUS DISEASE)

[About Release](#) [Back to the Top](#)

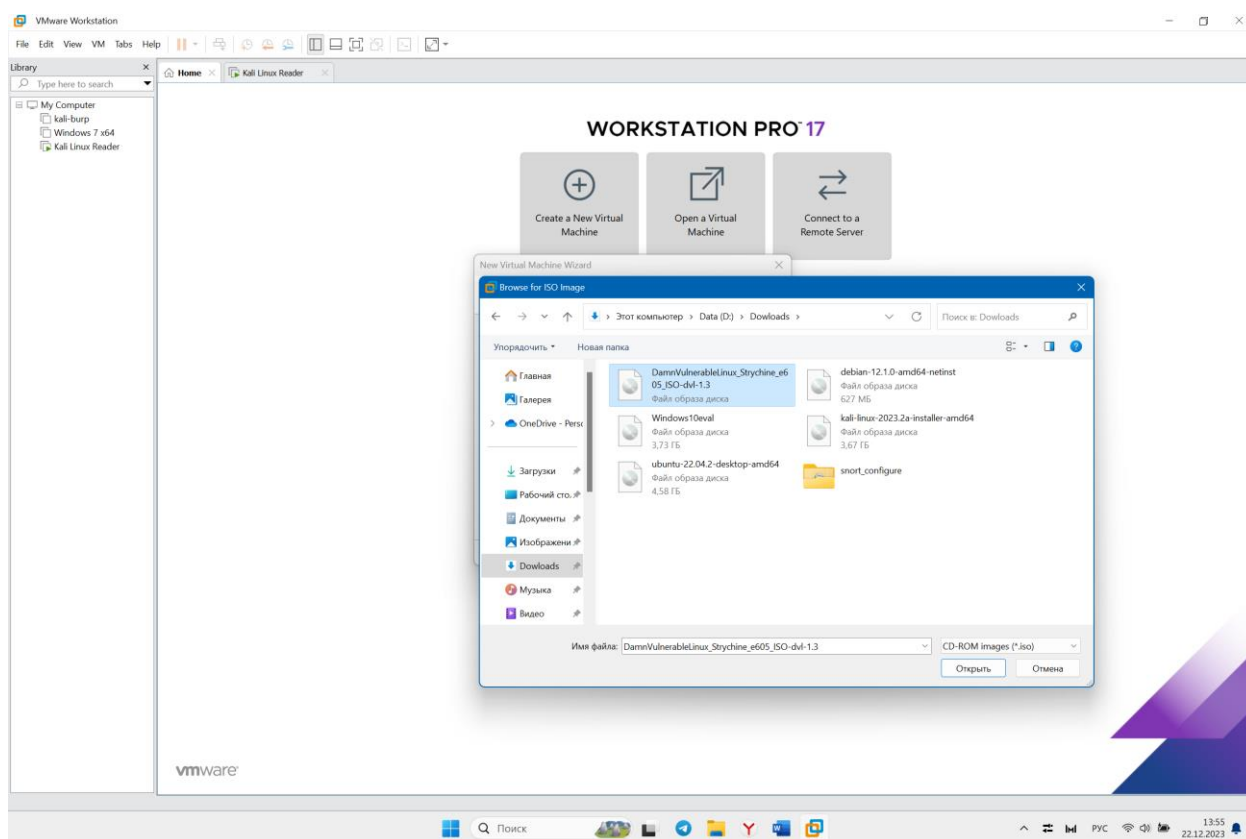
Name: Damn Vulnerable Linux (DVL): 1.5 (Infectious Disease)
Date release: 26 Jan 2009
Author: DVL
Series: Damn Vulnerable Linux (DVL)
Web page:
<http://web.archive.org/web/20090204172550/http://damnvulnerablelinux.org/index.php/eng/Damn%20Vulnerable%20Linux%20Distro/Damn%20Vulnerable%20Linux/Download>

[Download](#) [Back to the Top](#)

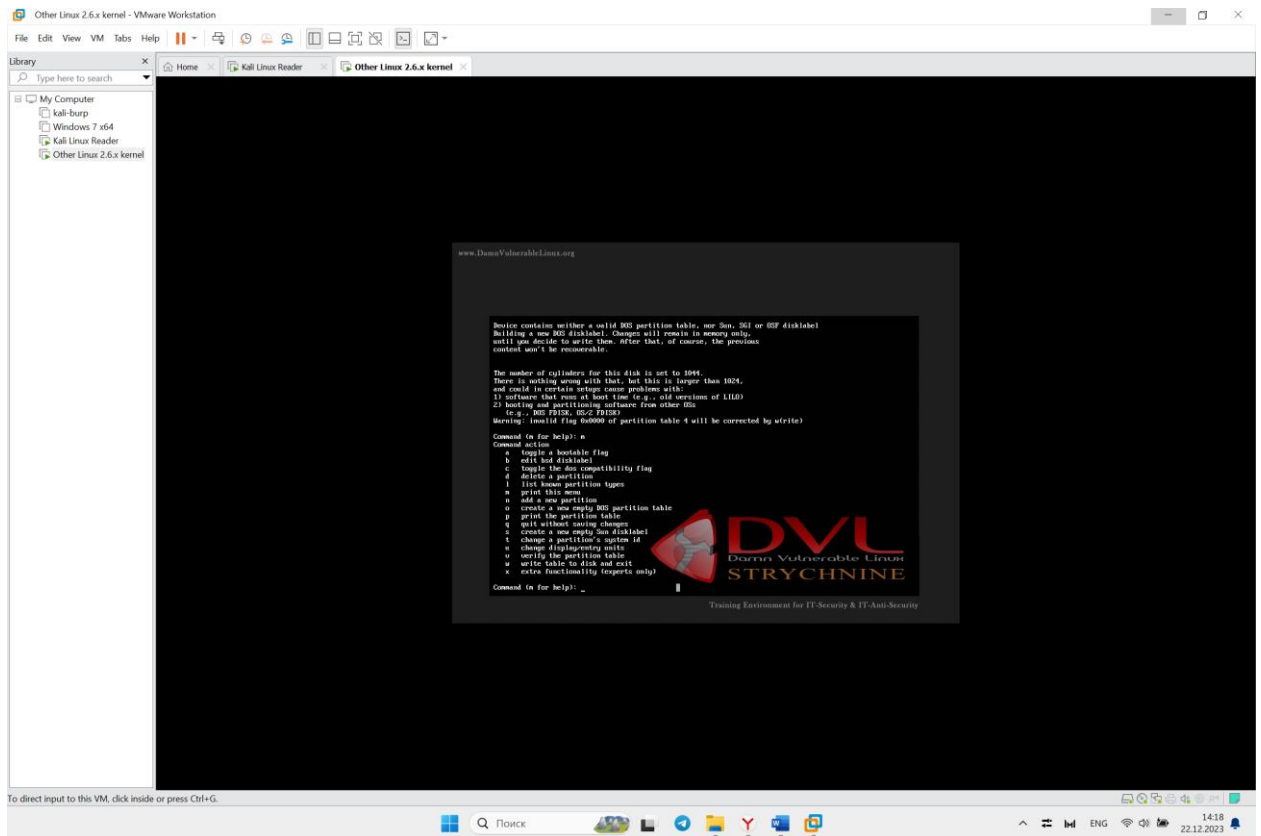
Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

DamnVulnerableLinux_Strychine_e605_ISO-dvl-1.3.iso (Size: 1.1 GB)
Download (Mirror): https://download.vulnhub.com/dvl/archive/DamnVulnerableLinux_Strychine_e605_ISO-dvl-1.3.iso

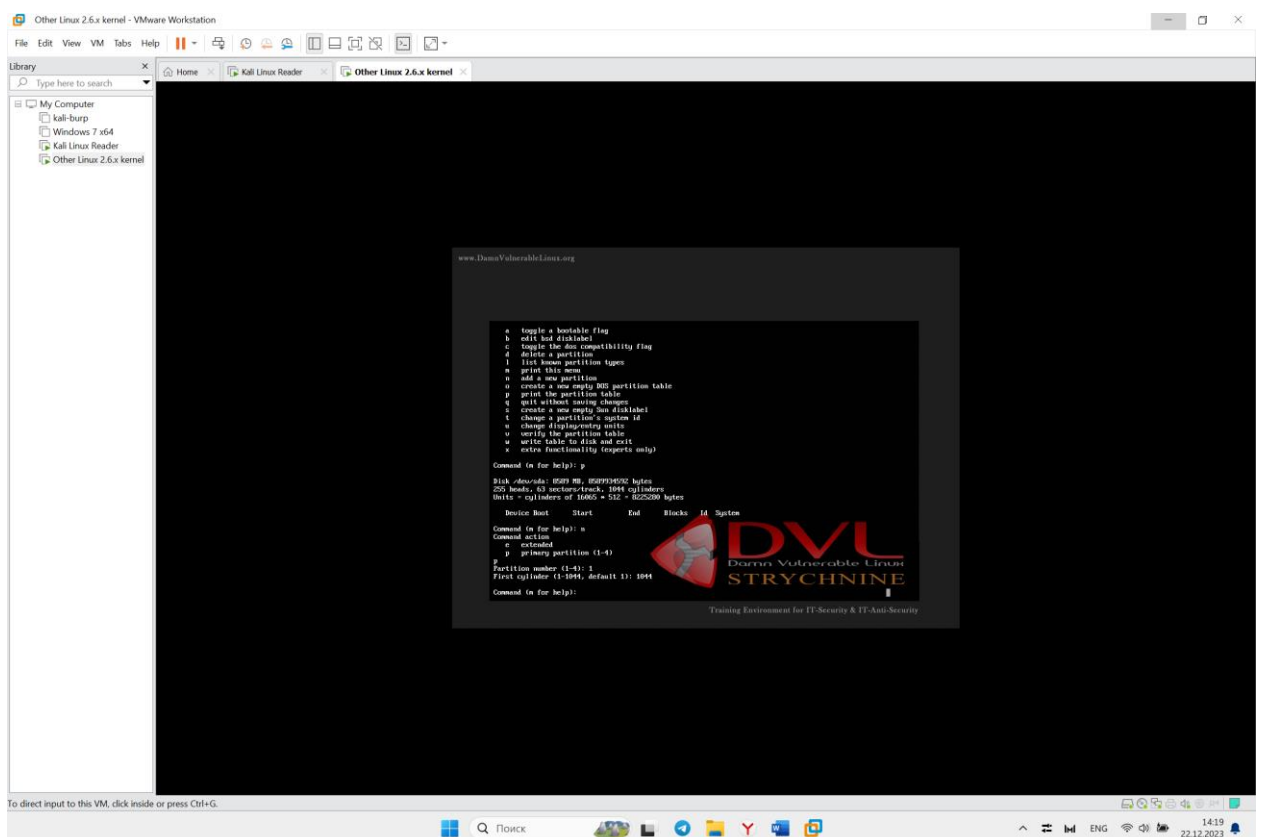
Выполним установку образа в VMWare.



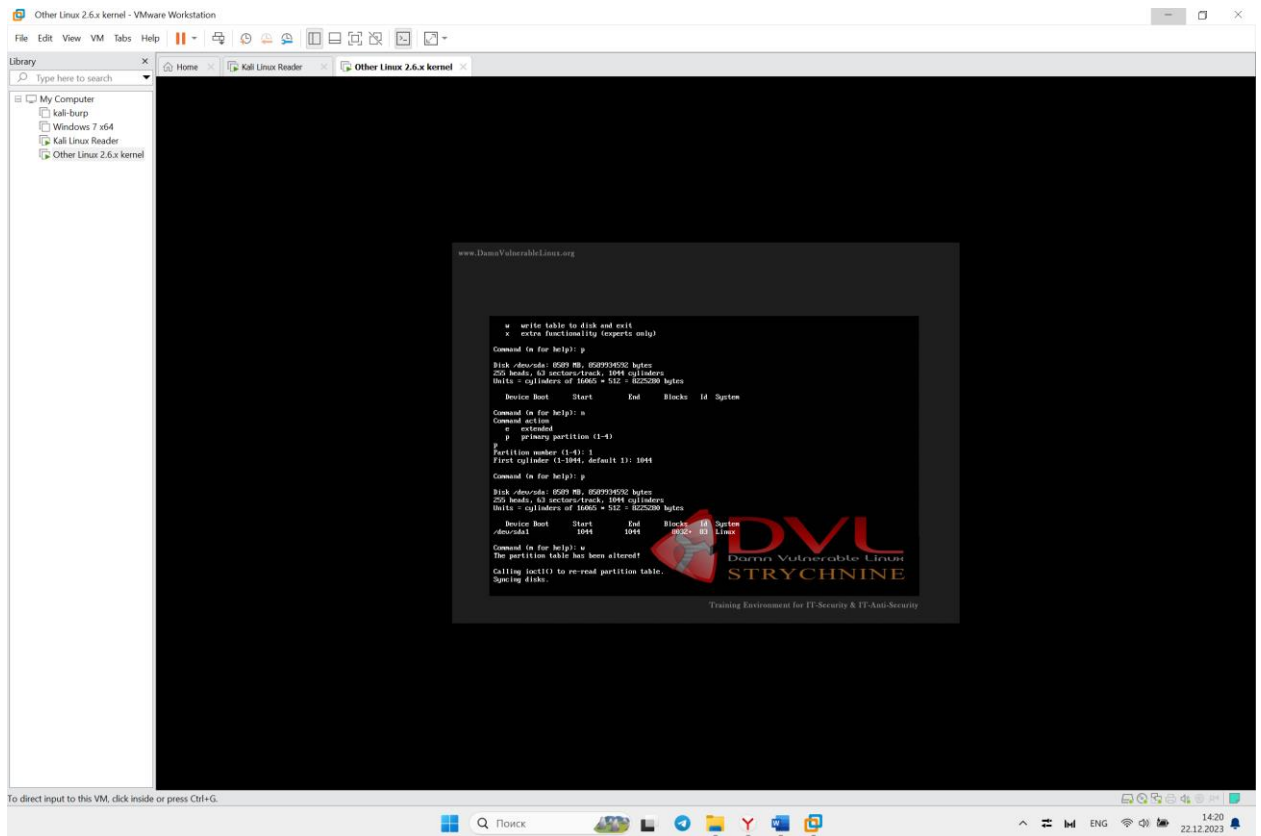
Выполняется загрузка ВМ.



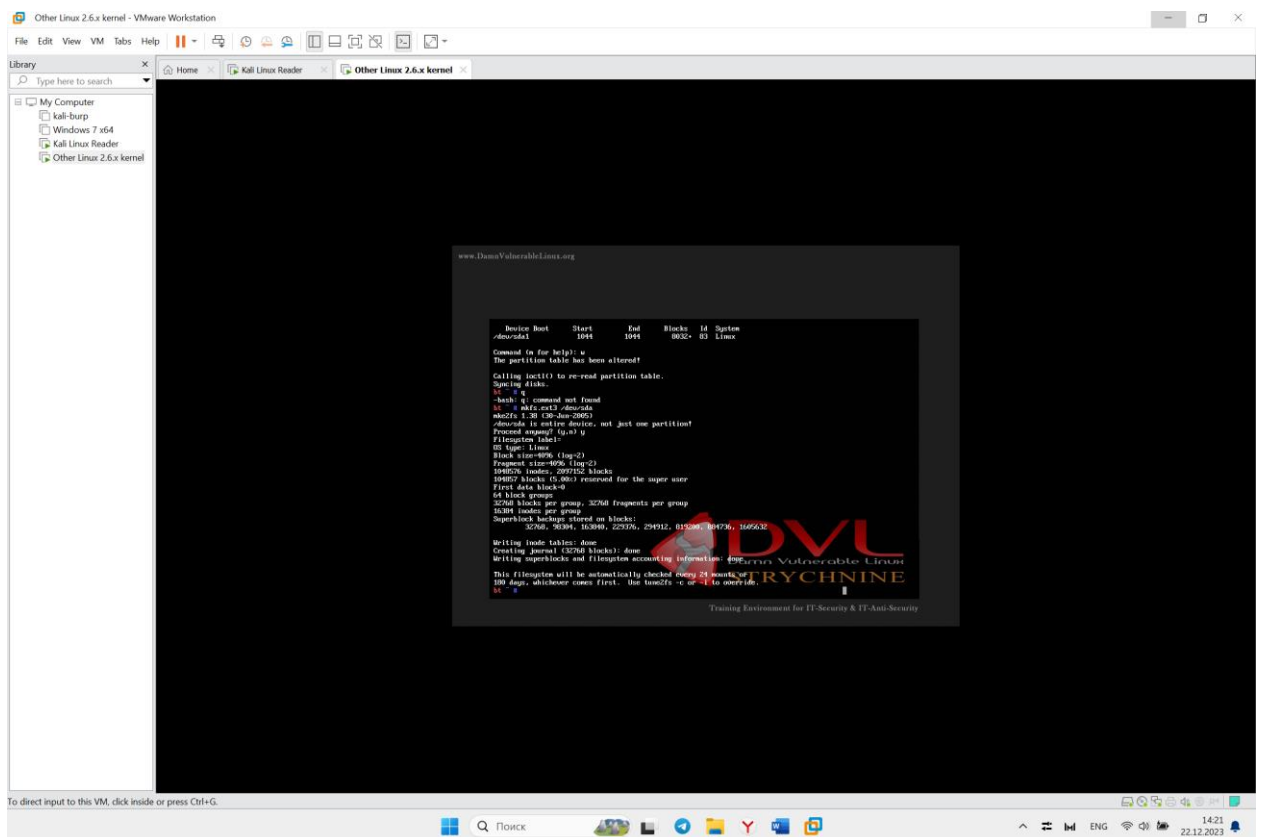
Выберем и создадим раздел.



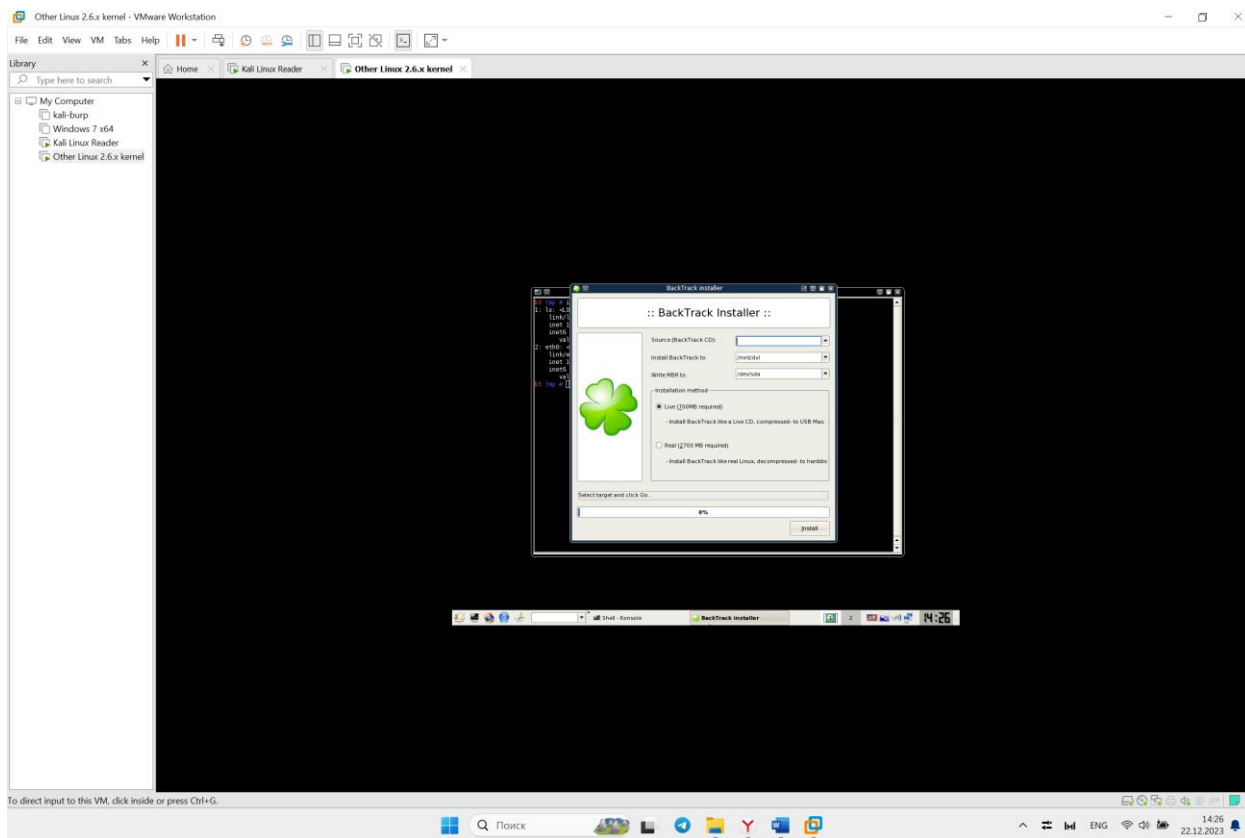
Просмотри созданный раздел.



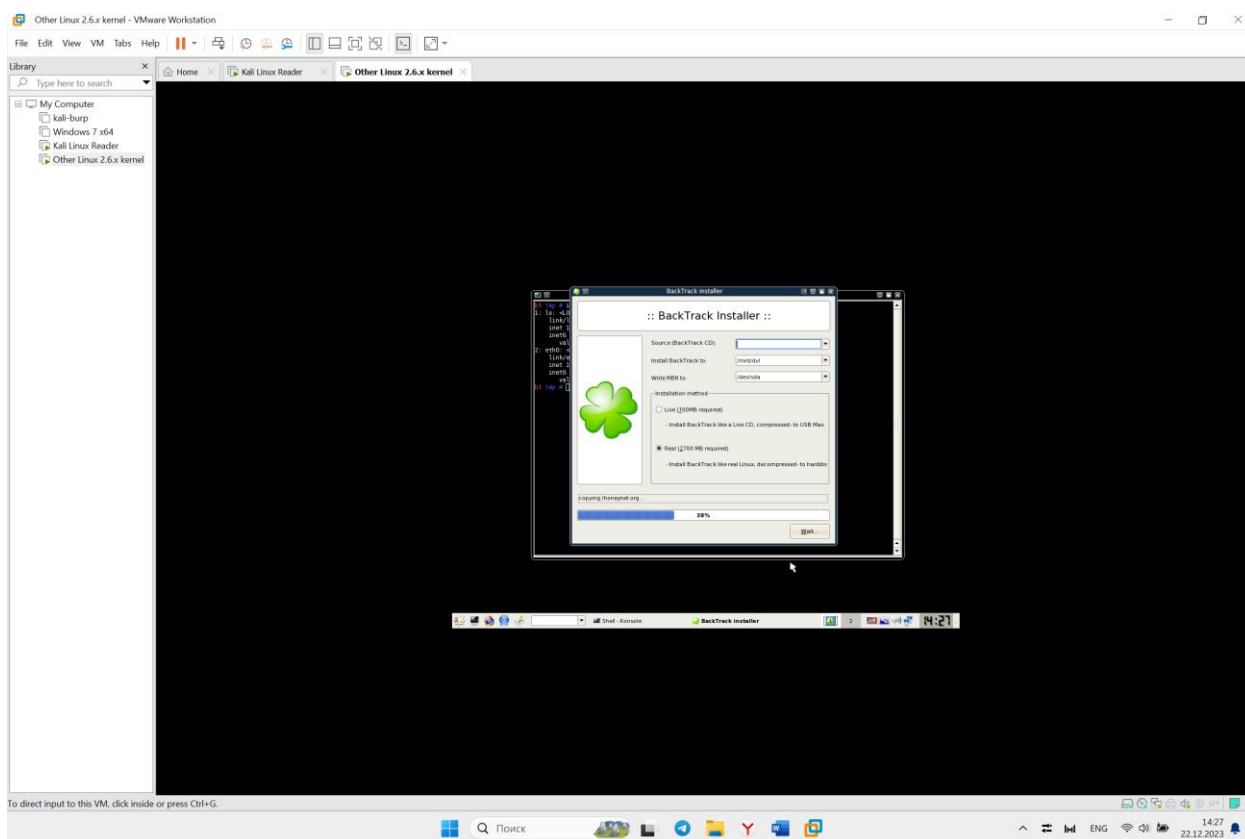
Отформатируем раздел.



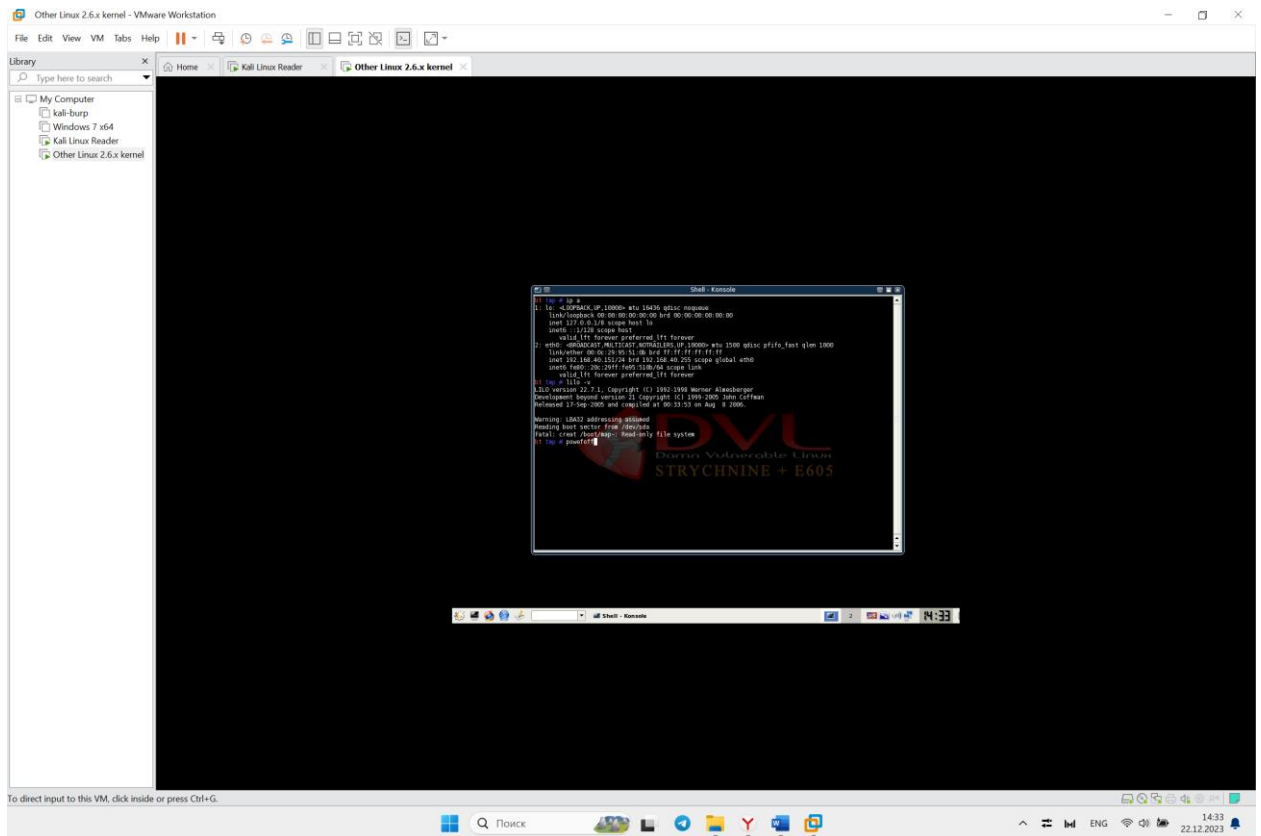
Создадим папку для монтирования раздела.



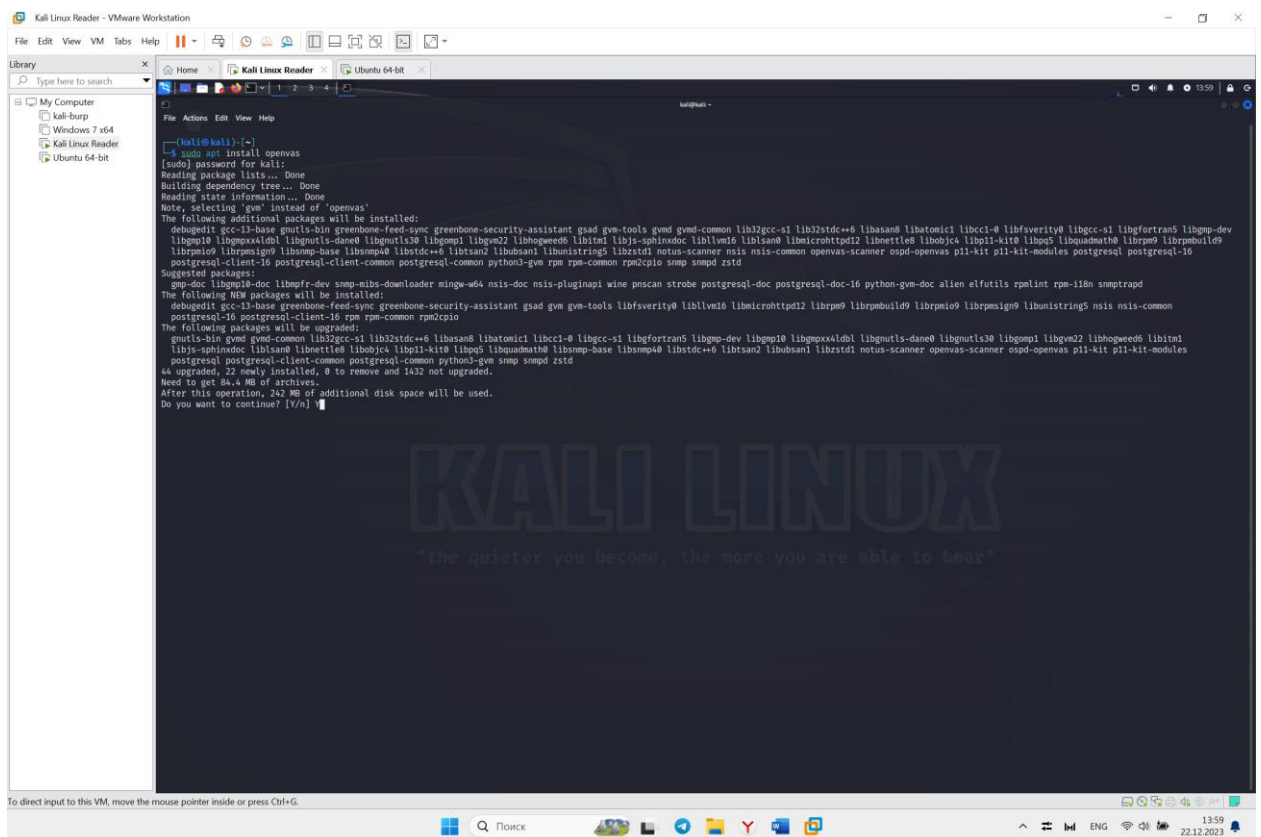
Выполняется процесс установки.



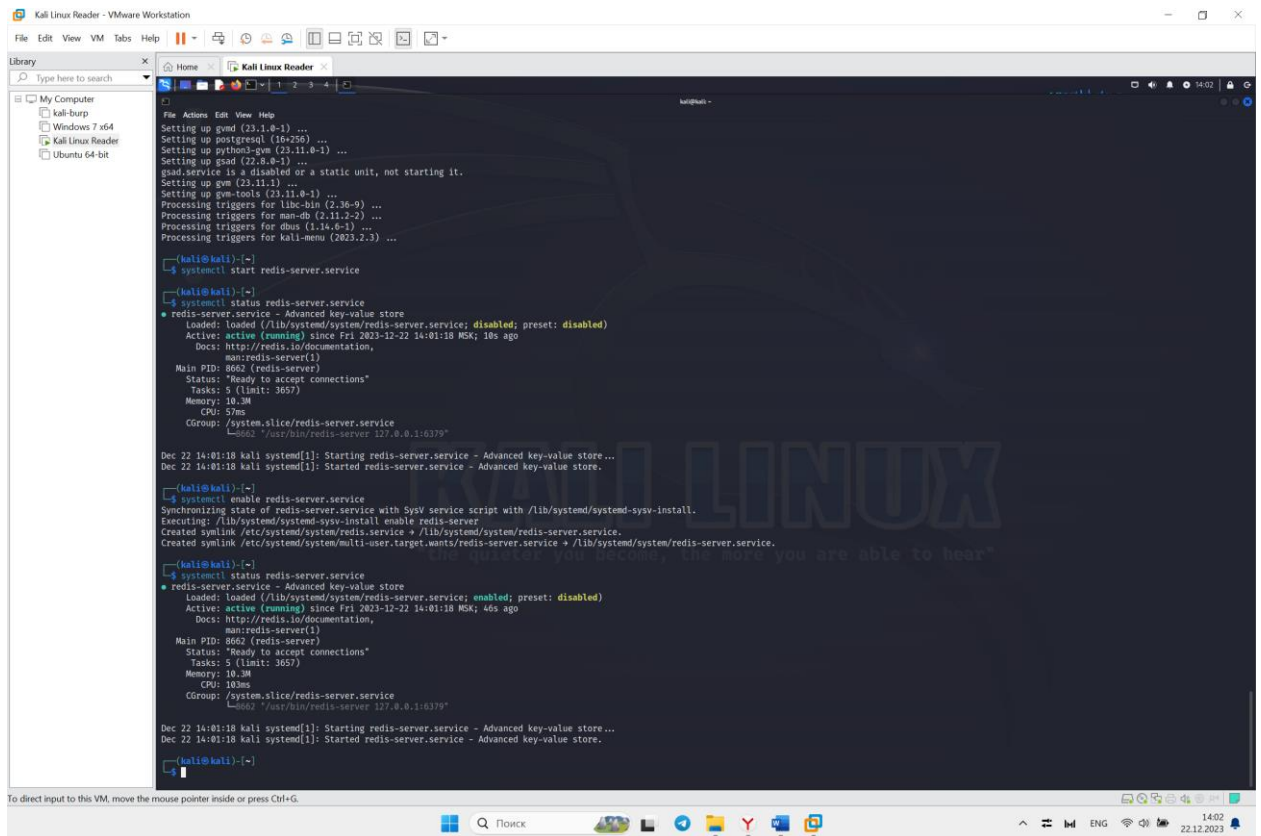
Установим загрузчик и выполним перезагрузку.



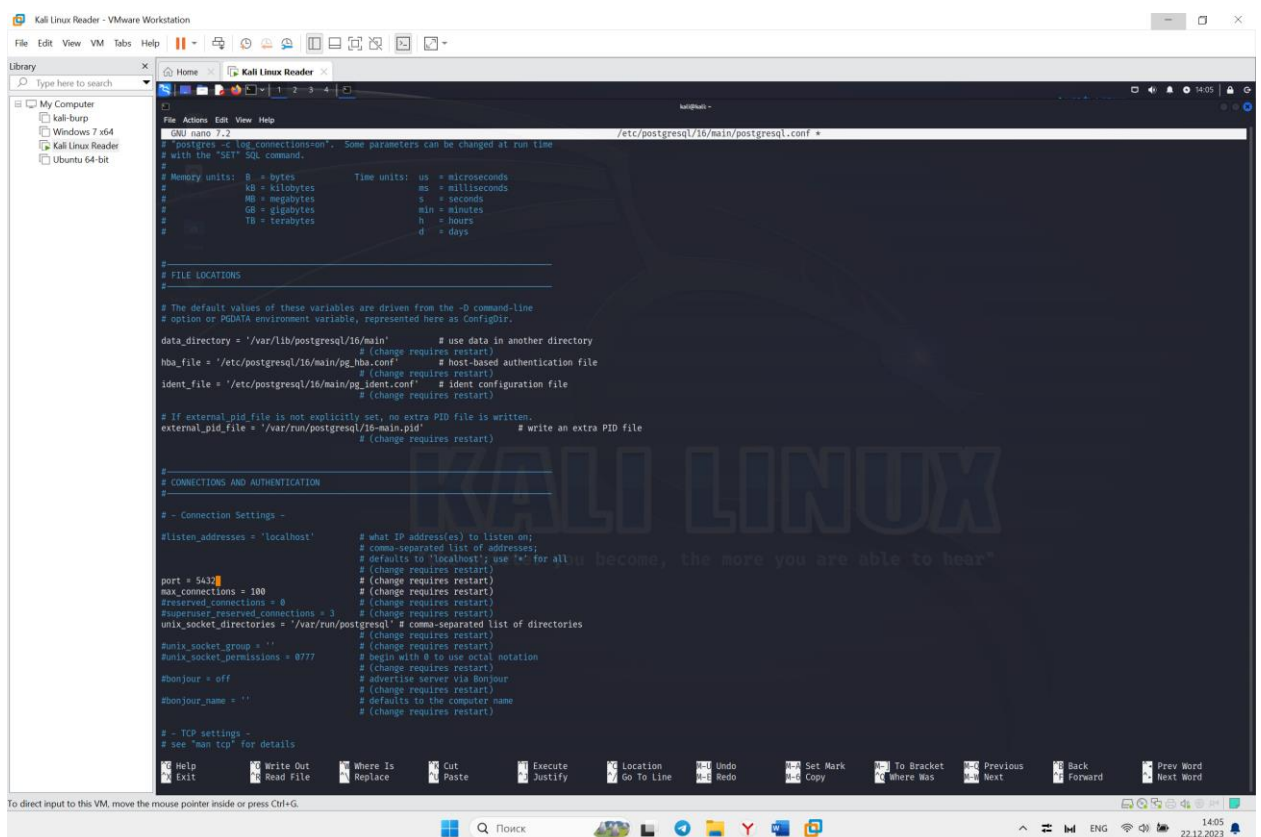
Установим OpenVas на уже имеющуюся VM Kali Linux.



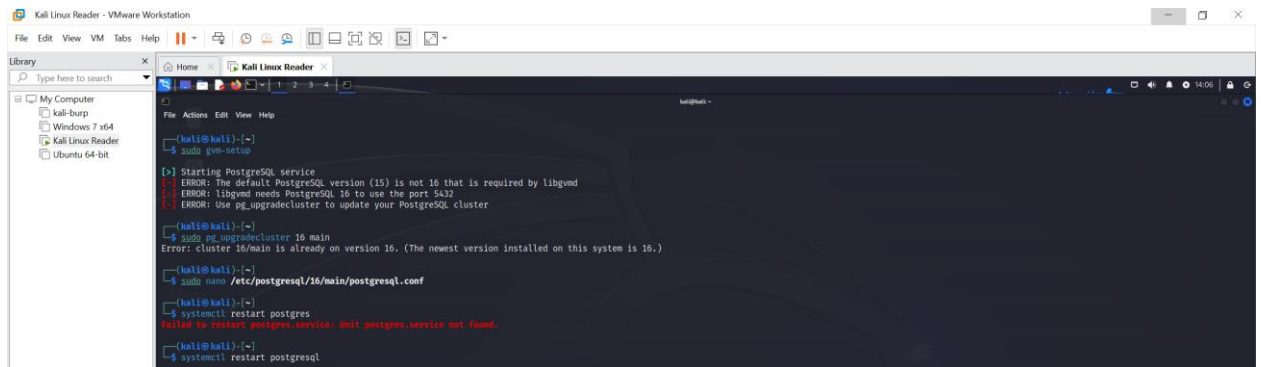
Запустим Redis.



Из-за ошибки PostgreSQL выполним изменение в конфигурационном файле.



Заново запустим загрузку OpenVas.



```
(kali@kali)~$ sudo gvm-setup
[+] Starting PostgreSQL service
[-] ERROR: The default PostgreSQL version (15) is not 16 that is required by libgvm
[-] ERROR: libgvm needs PostgreSQL 16 to use the port 5432
[-] ERROR: Use pg_upgradecluster to update your PostgreSQL cluster

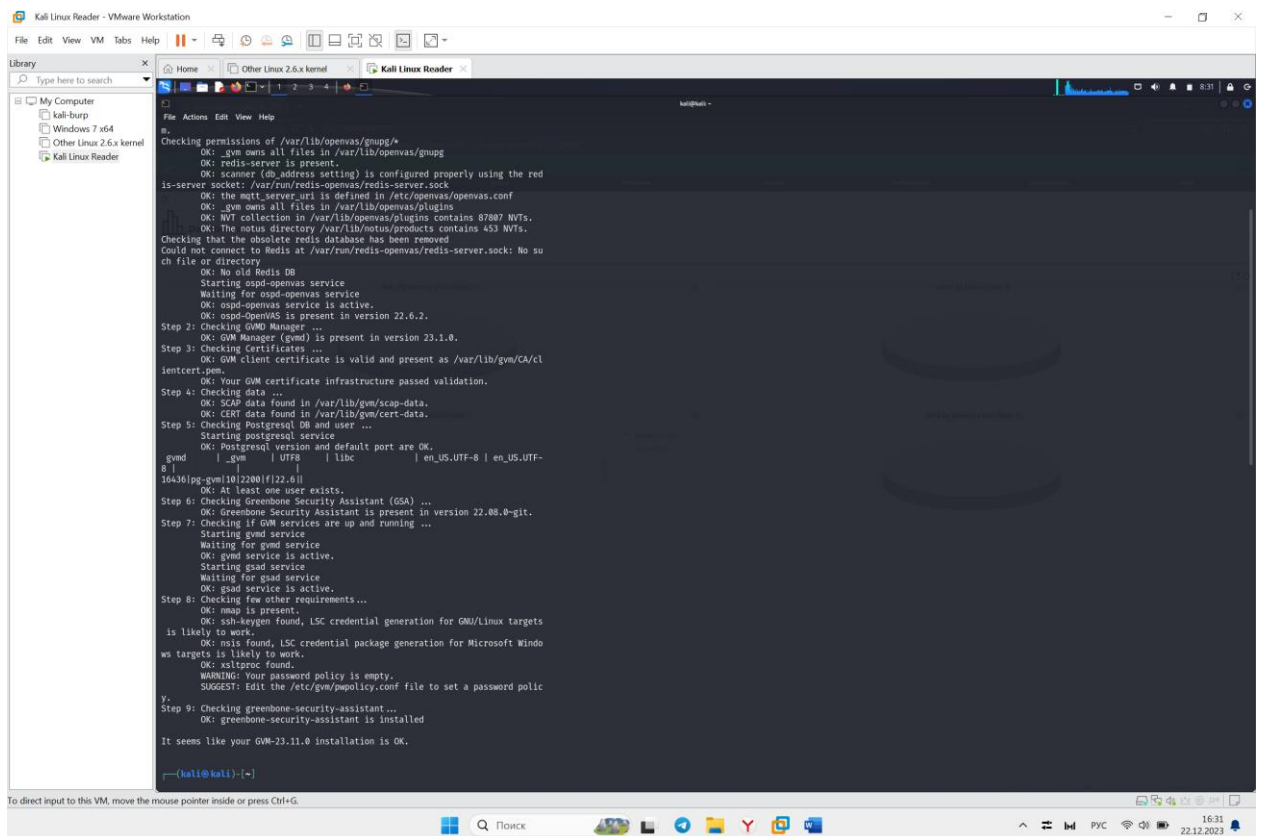
(kali@kali)~$ sudo pg_upgradecluster 16 main
Error: cluster 16/main is already on version 16. (The newest version installed on this system is 16.)

(kali@kali)~$ sudo nano /etc/postgresql/16/main/postgresql.conf

(kali@kali)~$ systemctl restart postgres
Failed to restart postgres.service: Unit postgres.service not found.

(kali@kali)~$ systemctl restart postgresql
```

Загрузка выполнена корректно, нам предоставлены данные для входа.

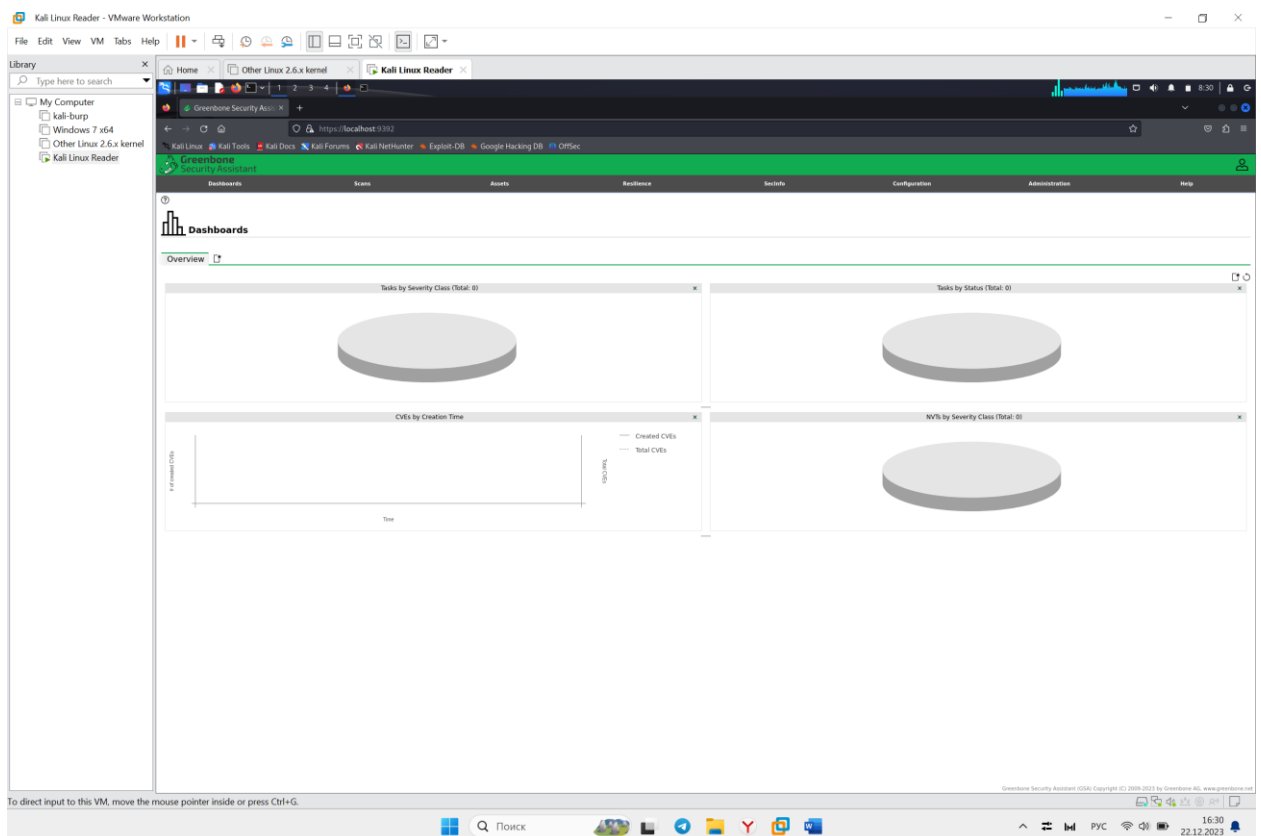
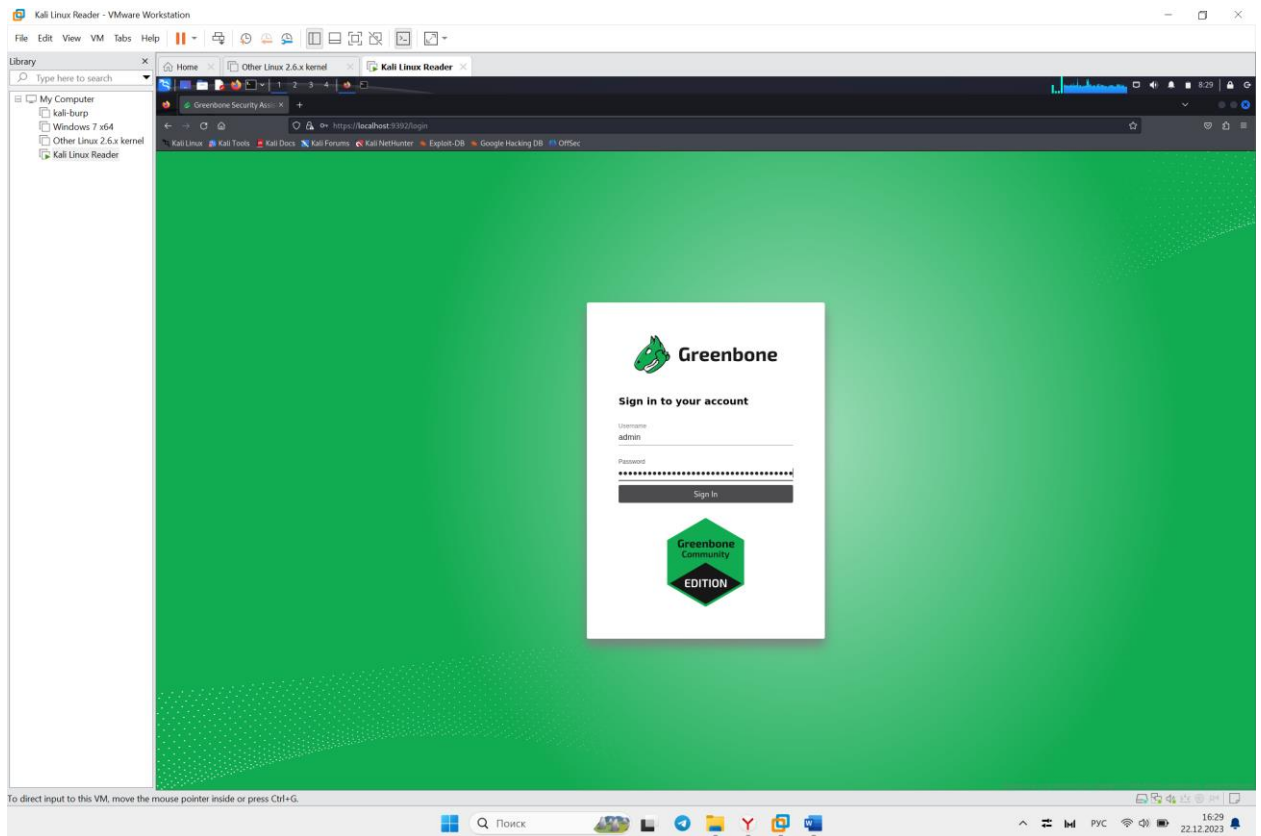


```
Checking permissions of /var/lib/openvas/gnupg/*
OK: gvm owns all files in /var/lib/openvas/gnupg
OK: redis-server is present.
OK: scanner (db_address setting) is configured properly using the red
is-server socket: /var/run/redis-openvas/redis-server.sock
OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
OK: gvm owns all files in /var/lib/openvas/plugins
OK: NVT collection in /var/lib/openvas/plugins contains 87807 NVTs.
OK: The notus directory /var/lib/notus/products contains 453 NVTs.
Checking that the obsolete redis database has been removed
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No su
ch file or directory
OK: No old Redis DB
Starting osdp-openvas service
Waiting for osdp-openvas service
OK: osdp-openvas service is active.
OK: osdp-openvas is present in version 22.6.2.
Step 2: Checking GVM Manager ...
OK: GVM Manager (gvm) is present in version 23.1.0.
Step 3: Checking Certificates ...
OK: GVM client certificate is valid and present as /var/lib/gvm/CA/cl
ientcert.pem.
OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data ...
OK: SCAP data found in /var/lib/gvm/scap-data.
OK: CERT data found in /var/lib/gvm/cert-data.
Step 5: Checking PostgreSQL DB and user ...
Starting postgresql service
OK: postgresql version and default port are OK.
gvm | _gvm | UTF8 | libc | en_US.UTF-8 | en_US.UTF-
8 |
16436/pg-gvm10122000f122.611
OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
OK: Greenbone Security Assistant is present in version 22.08.0-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, ISC credential generation for GNU/Linux targets
is likely to work.
OK: nsis found, ISC credential package generation for Microsoft Windo
ws targets is likely to work.
OK: xsltproc found.
WARNING: Your password policy is empty.
SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password polic
y.
Step 9: Checking greenbone-security-assistant...
OK: greenbone-security-assistant is installed
It seems like your GVM-23.11.0 installation is OK.

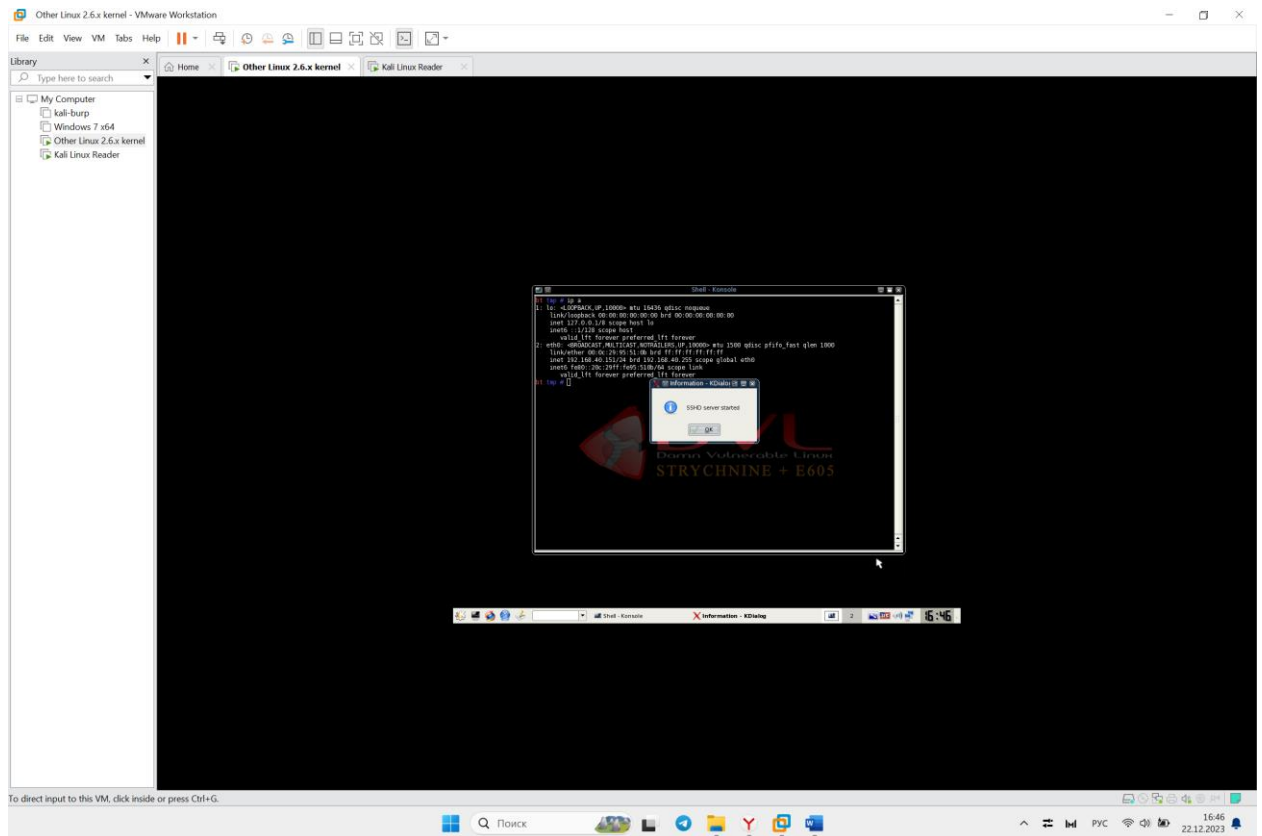
(kali@kali)~$
```

Please note the generated admin password

[*] User created with password '85783b0a-3459-4bb2-8f92-225d70fbfa49'.

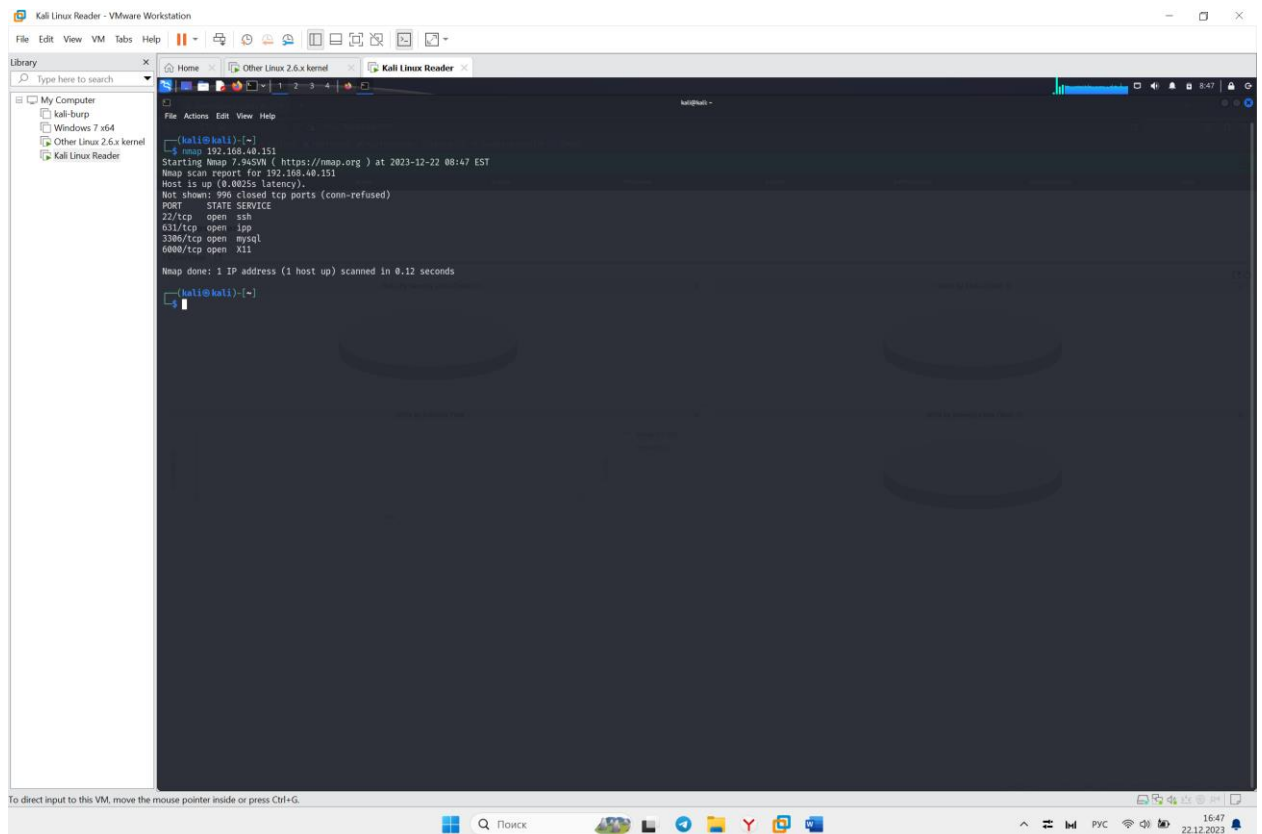


Обновим БД.

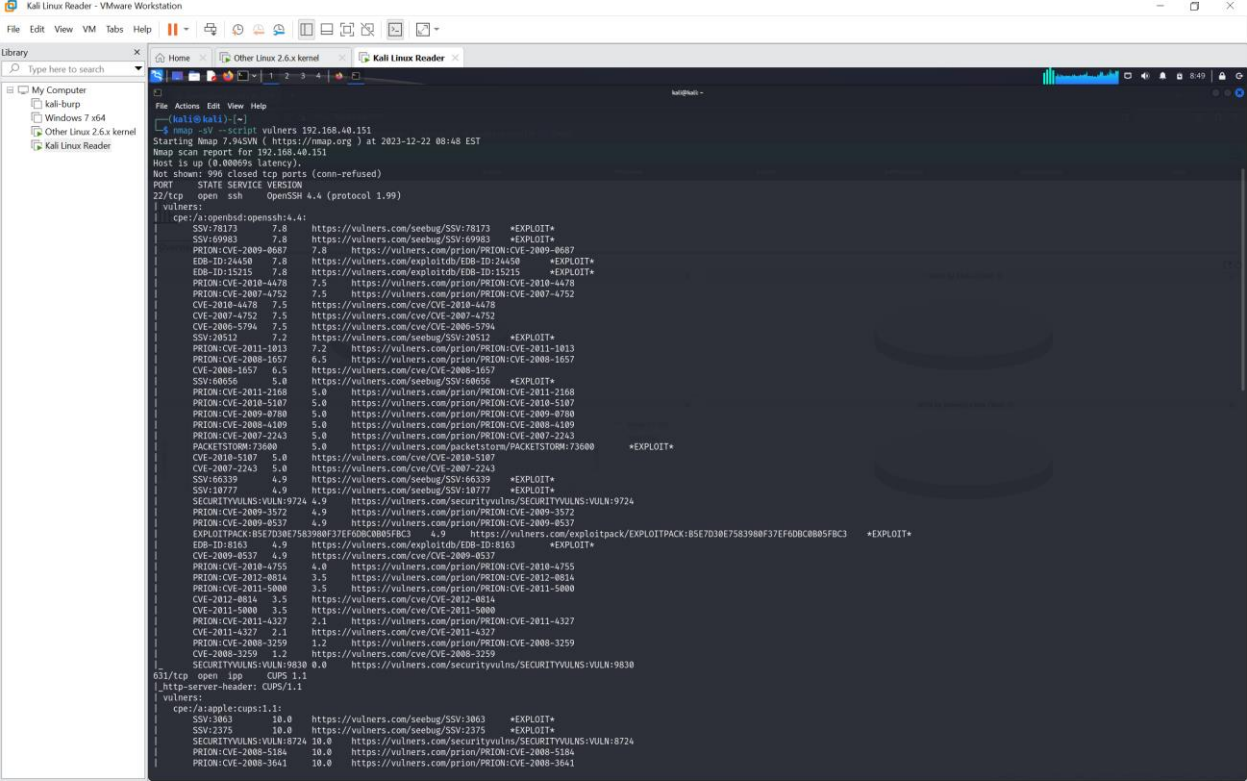


Задание 2. Сканирование сети и уязвимостей.

Выполним сканирование ВМ с помощью nmap.

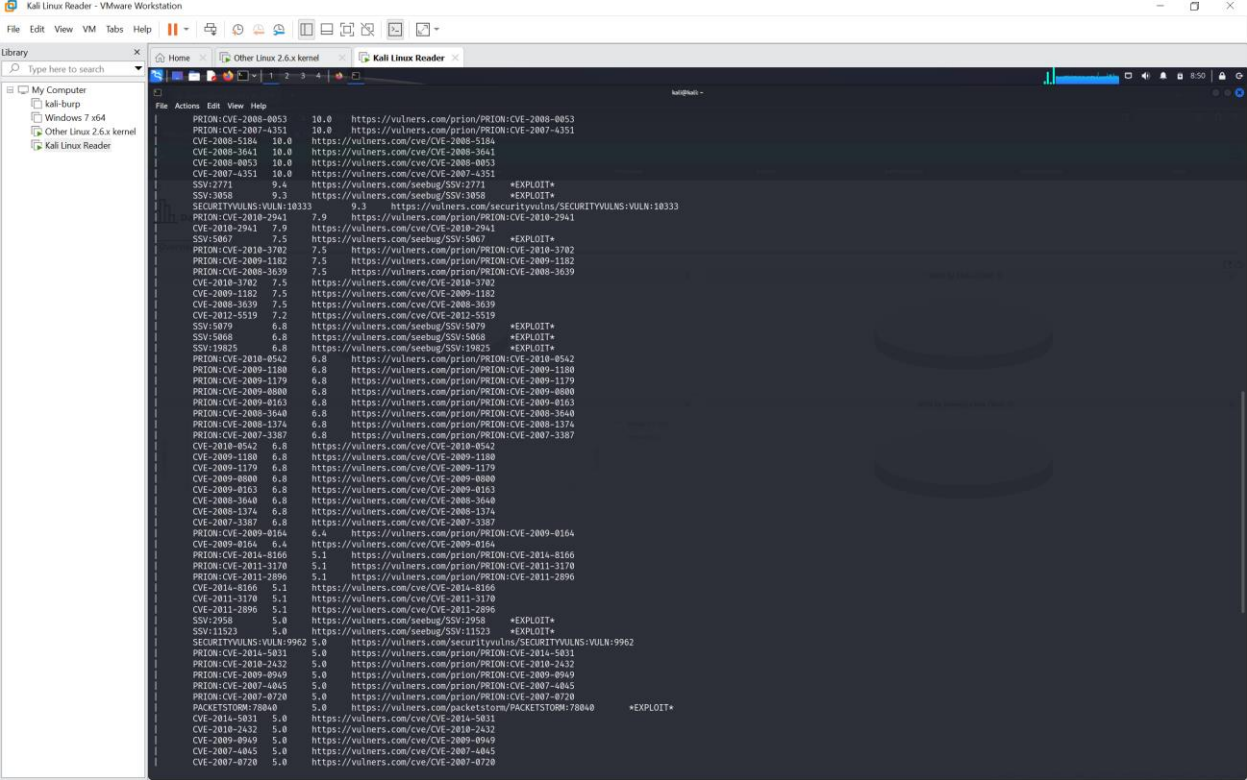


Воспользуемся надстройкой в nmap, запустим дополнительный тип сканирования на наличие уязвимостей.



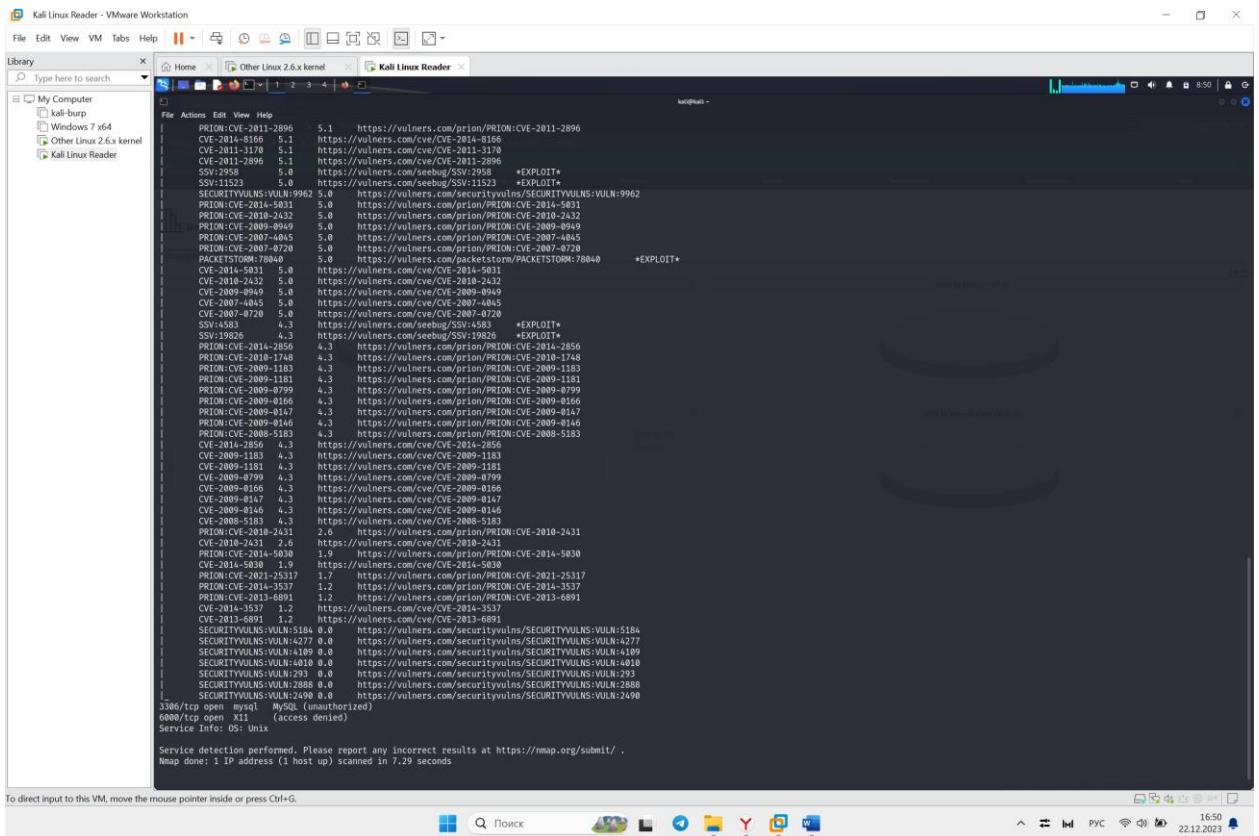
The screenshot shows a Kali Linux Reader virtual machine running nmap. The terminal output displays the results of a scan on 192.168.40.151, including host information, open ports (SSH), and a detailed list of detected vulnerabilities. The vulnerabilities are categorized by severity (e.g., 7.8, 5.0, 10.0) and include links to CVE entries and exploit databases. The scan was performed using the --script=vulners option.

```
[kali@kali]~$ nmap -sV --script=vulners 192.168.40.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-22 08:40 EST
Nmap scan report for 192.168.40.151
Host is up (0.00069s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.4 (protocol 1.99)
|_ vulners:
|_ cpe:/a:openssl:openssl:4.4.1:
|_ SSV:78173 7.8 https://vulners.com/seebug/SSV:78173 *EXPLOIT+
|_ SSV:69983 7.8 https://vulners.com/seebug/SSV:69983 *EXPLOIT+
|_ PRION:CVE-2009-4047 7.8 https://vulners.com/prion/PRION:CVE-2009-4047
|_ 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
|_ CVE-2007-4752 7.5 https://vulners.com/cve/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-2011-1013 7.2 https://vulners.com/prion/PRION:CVE-2011-1013
|_ CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657
|_ SSV:60650 5.0 https://vulners.com/seebug/SSV:60650 *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-2009-4700 5.0 https://vulners.com/prion/PRION:CVE-2009-4700
|_ 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:65359 4.9 https://vulners.com/seebug/SSV:65359 *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-2009-4037 4.9 https://vulners.com/prion/PRION:CVE-2009-4037
|_ EXPLOITPACK:B5E7D30E7583980F37EF60CB0B5F8C3 4.9 https://vulners.com/exploitpack/EXPLOITPACK:B5E7D30E7583980F37EF60CB0B5F8C3 *EXPLOIT+
|_ EDB-ID:8163 4.9 https://vulners.com/exploitdb/EDB-ID:8163 *EXPLOIT+
|_ CVE-2009-4037 4.9 https://vulners.com/cve/CVE-2009-4037
|_ 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
|_ CVE-2011-5000 3.5 https://vulners.com/cve/CVE-2011-5000
|_ CVE-2012-0814 3.5 https://vulners.com/cve/CVE-2012-0814
|_ PRION:CVE-2011-5000 2.1 https://vulners.com/prion/PRION:CVE-2011-5000
|_ 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
|_ 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
```

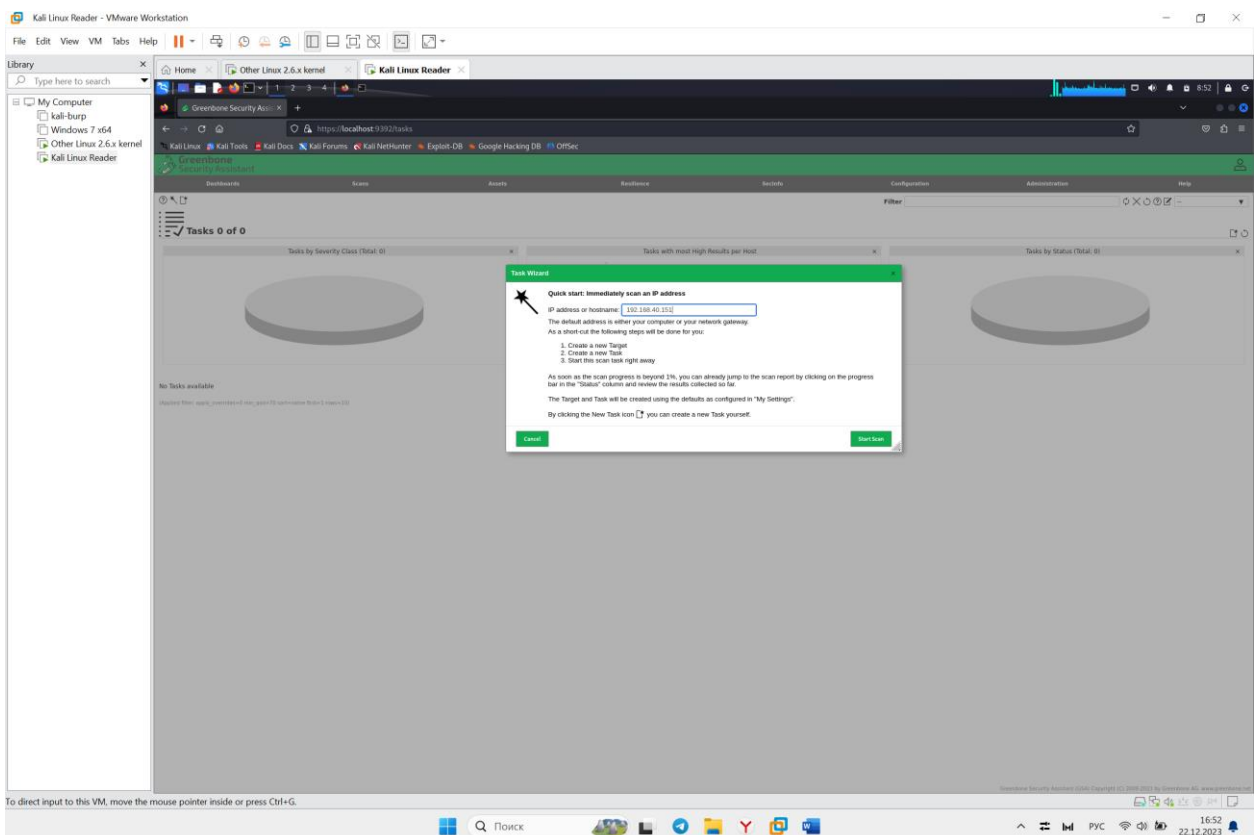


This screenshot continues the nmap scan results from the previous image, showing a large number of detected vulnerabilities. The list includes various CVEs and their associated severity scores, as well as links to exploit databases and security advisories. The scan continues to identify weaknesses in the system's configuration and software components.

```
|_ 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:18333 9.3 https://vulners.com/securityvulns/SECURITYVULNS:VULN:18333
|_ 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
|_ CVE-2009-1182 7.5 https://vulners.com/cve/CVE-2009-1182
|_ CVE-2008-3639 7.5 https://vulners.com/cve/CVE-2008-3639
|_ CVE-2012-5519 7.2 https://vulners.com/cve/CVE-2012-5519
|_ SSV:5079 6.8 https://vulners.com/seebug/SSV:5079 *EXPLOIT+
|_ SSV:5068 6.8 https://vulners.com/seebug/SSV:5068 *EXPLOIT+
|_ SSV:10025 6.8 https://vulners.com/seebug/SSV:10025 *EXPLOIT+
|_ PRION:CVE-2010-0542 6.8 https://vulners.com/prion/PRION:CVE-2010-0542
|_ PRION:CVE-2009-1180 6.8 https://vulners.com/prion/PRION:CVE-2009-1180
|_ PRION:CVE-2009-1179 6.8 https://vulners.com/prion/PRION:CVE-2009-1179
|_ PRION:CVE-2009-0800 6.8 https://vulners.com/prion/PRION:CVE-2009-0800
|_ PRION:CVE-2009-0163 6.8 https://vulners.com/prion/PRION:CVE-2009-0163
|_ PRION:CVE-2008-3640 6.8 https://vulners.com/prion/PRION:CVE-2008-3640
|_ PRION:CVE-2008-1374 6.8 https://vulners.com/prion/PRION:CVE-2008-1374
|_ PRION:CVE-2007-3387 6.8 https://vulners.com/prion/PRION:CVE-2007-3387
|_ CVE-2010-0542 6.8 https://vulners.com/cve/CVE-2010-0542
|_ CVE-2009-1180 6.8 https://vulners.com/cve/CVE-2009-1180
|_ CVE-2009-1179 6.8 https://vulners.com/cve/CVE-2009-1179
|_ CVE-2009-0800 6.8 https://vulners.com/cve/CVE-2009-0800
|_ CVE-2009-0163 6.8 https://vulners.com/cve/CVE-2009-0163
|_ CVE-2008-3640 6.8 https://vulners.com/cve/CVE-2008-3640
|_ CVE-2008-1374 6.8 https://vulners.com/cve/CVE-2008-1374
|_ CVE-2007-3387 6.8 https://vulners.com/cve/CVE-2007-3387
|_ PRION:CVE-2009-0164 6.4 https://vulners.com/prion/PRION:CVE-2009-0164
|_ CVE-2009-0164 6.4 https://vulners.com/cve/CVE-2009-0164
|_ PRION:CVE-2014-8166 5.1 https://vulners.com/prion/PRION:CVE-2014-8166
|_ PRION:CVE-2011-3170 5.1 https://vulners.com/prion/PRION:CVE-2011-3170
|_ PRION:CVE-2011-2896 5.1 https://vulners.com/prion/PRION:CVE-2011-2896
|_ CVE-2014-8166 5.1 https://vulners.com/cve/CVE-2014-8166
|_ CVE-2011-3170 5.1 https://vulners.com/cve/CVE-2011-3170
|_ CVE-2011-2896 5.1 https://vulners.com/cve/CVE-2011-2896
|_ SSV:2958 5.0 https://vulners.com/seebug/SSV:2958 *EXPLOIT+
|_ SSV:11523 5.0 https://vulners.com/seebug/SSV:11523 *EXPLOIT+
|_ SECURITYVULNS:VULN:9962 5.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:9962
|_ PRION:CVE-2014-5031 5.0 https://vulners.com/prion/PRION:CVE-2014-5031
|_ PRION:CVE-2010-2432 5.0 https://vulners.com/prion/PRION:CVE-2010-2432
|_ PRION:CVE-2009-0949 5.0 https://vulners.com/prion/PRION:CVE-2009-0949
|_ PRION:CVE-2007-4045 5.0 https://vulners.com/prion/PRION:CVE-2007-4045
|_ PRION:CVE-2007-0720 5.0 https://vulners.com/prion/PRION:CVE-2007-0720
|_ PACKETSTORM:78040 5.0 https://vulners.com/packetstorm/PACKETSTORM:78040 *EXPLOIT+
|_ CVE-2014-5031 5.0 https://vulners.com/cve/CVE-2014-5031
|_ CVE-2010-2432 5.0 https://vulners.com/cve/CVE-2010-2432
|_ CVE-2009-0949 5.0 https://vulners.com/cve/CVE-2009-0949
|_ CVE-2007-4045 5.0 https://vulners.com/cve/CVE-2007-4045
|_ CVE-2007-0720 5.0 https://vulners.com/cve/CVE-2007-0720
```



Выполним сканирование с помощью OpenVas.



Просмотрим результаты сканирования.

Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Me
	(7 of 59)	(1 of 2)	(1 of 3)	(5 of 5)	(1 of 2)	(2 of 2)	(0 of 0)	(0 of 0)	(0 of 0)

Vulnerability	Severity	QoD
Deprecated SSH-1 Protocol Detection	7.5 (High)	80 %
Weak Host Key Algorithm(s) (SSH)	6.3 (Medium)	80 %
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	6.3 (Medium)	80 %
Weak Encryption Algorithm(s) Supported (SSH)	6.3 (Medium)	80 %
Weak MAC Algorithm(s) Supported (SSH)	6.3 (Medium)	80 %
TCP Timestamps Information Disclosure	2.5 (Low)	80 %
ICMP Timestamp Reply Information Disclosure	2.5 (Low)	80 %

(Applied filter: apply_severities=0 levels=low rows=100 min_row=70 first=1 sort=reverse=severity)

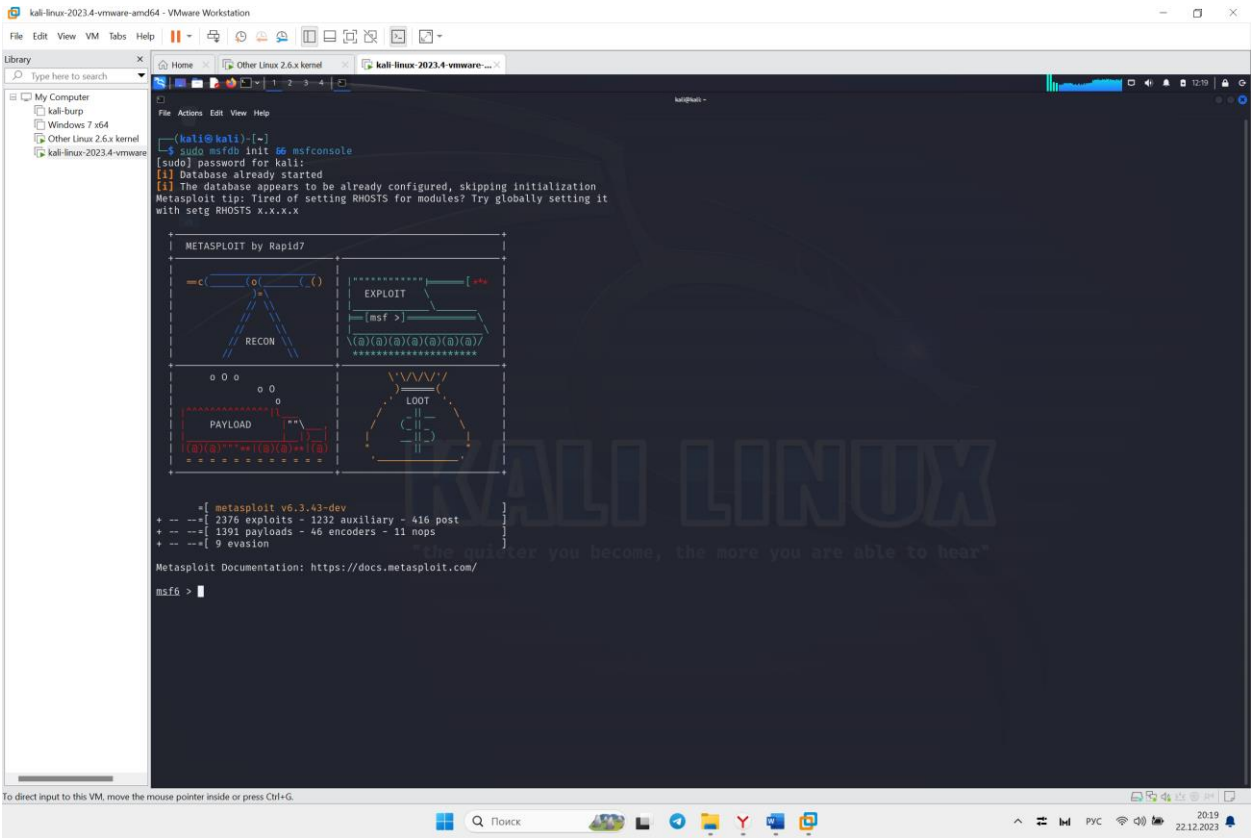
Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
	(7 of 59)	(1 of 2)	(1 of 3)	(5 of 5)	(1 of 2)	(2 of 2)	(0 of 0)	(0 of 0)	(0 of 0)	(0)

CVE	NVT	Hosts	Occurrences	Severity
CVE-2001-0361 CVE-2001-0572 CVE-2001-1473	Deprecated SSH-1 Protocol Detection	1	1	7.5 (High)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	1	1	2.5 (Low)

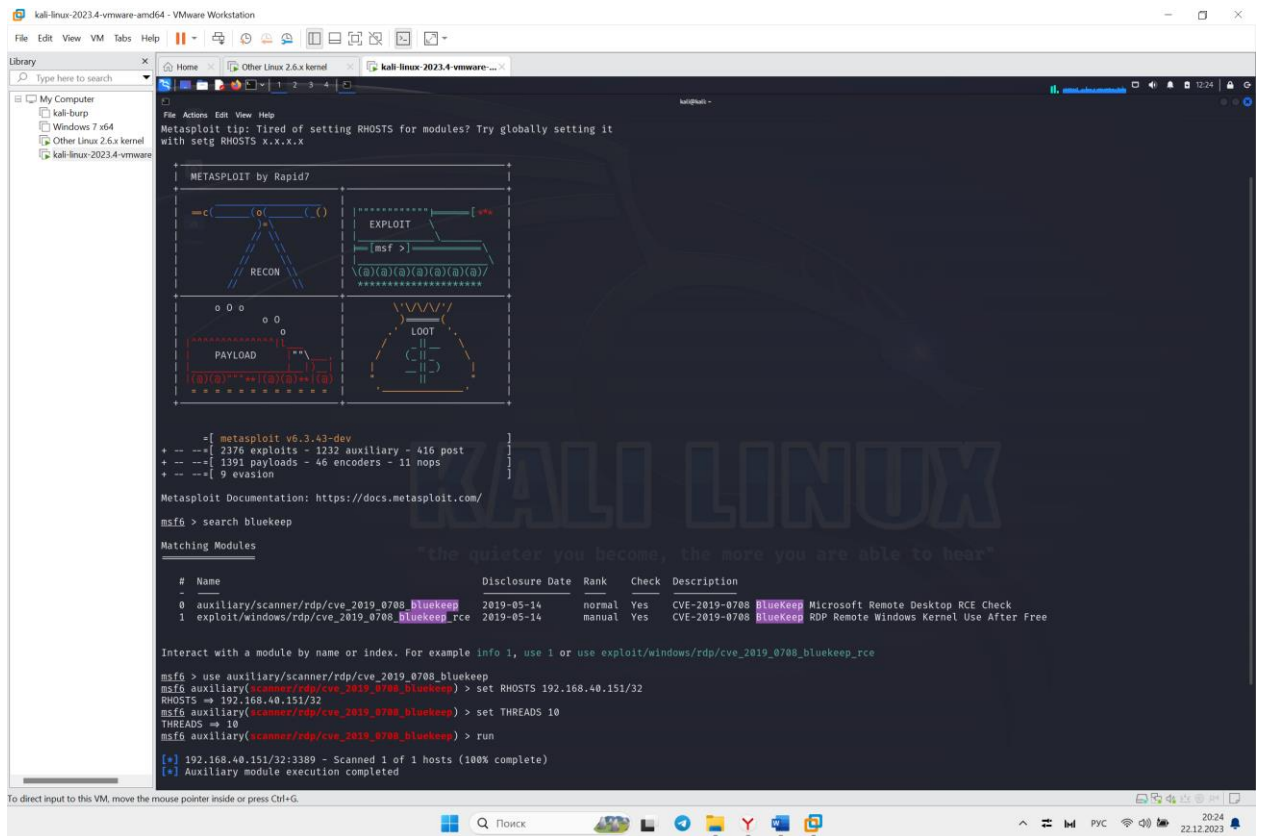
Из-за небольших возможностей openvas результат получился не таким наполненным и подробным, как у nmap.

Задание 3. Анализ безопасности системы.

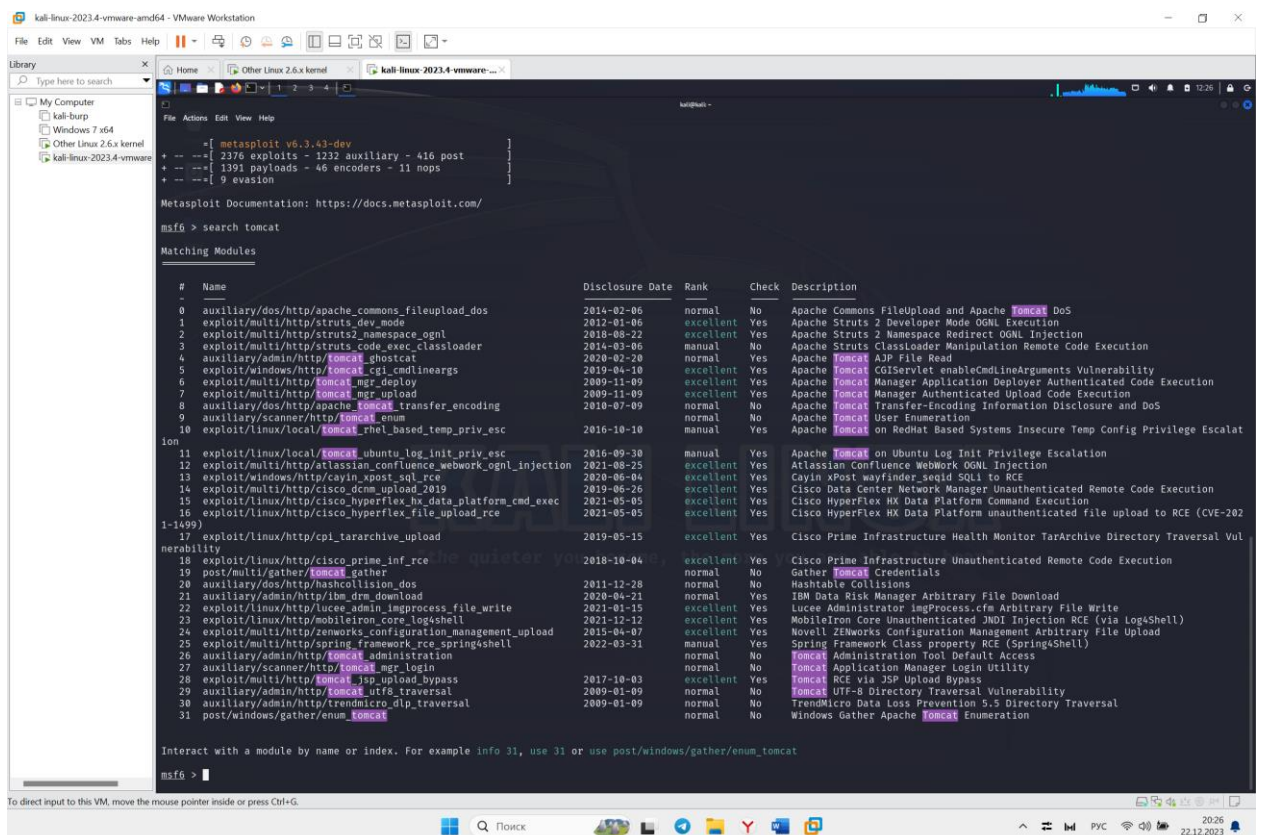
Выполним загрузку Metasploit.



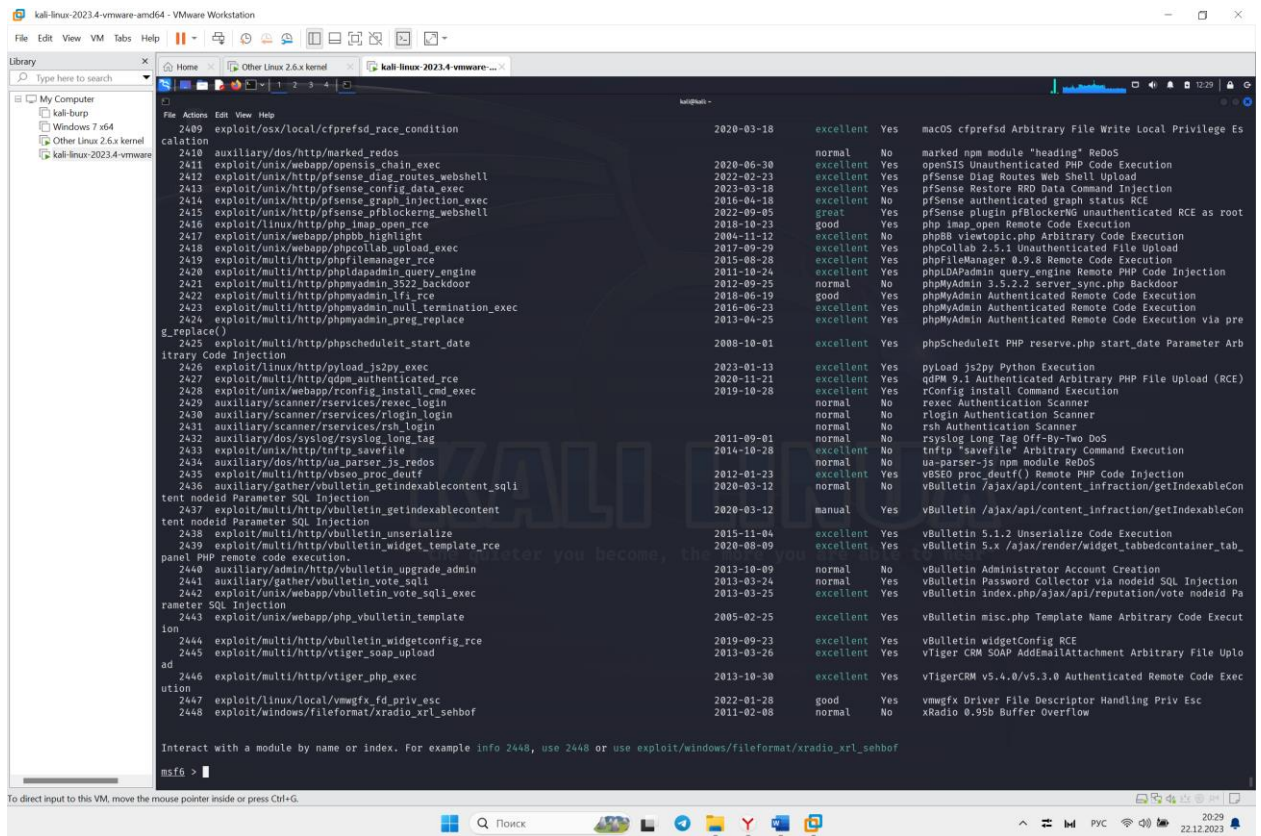
Выполним поиск и настройку BlueKeep.



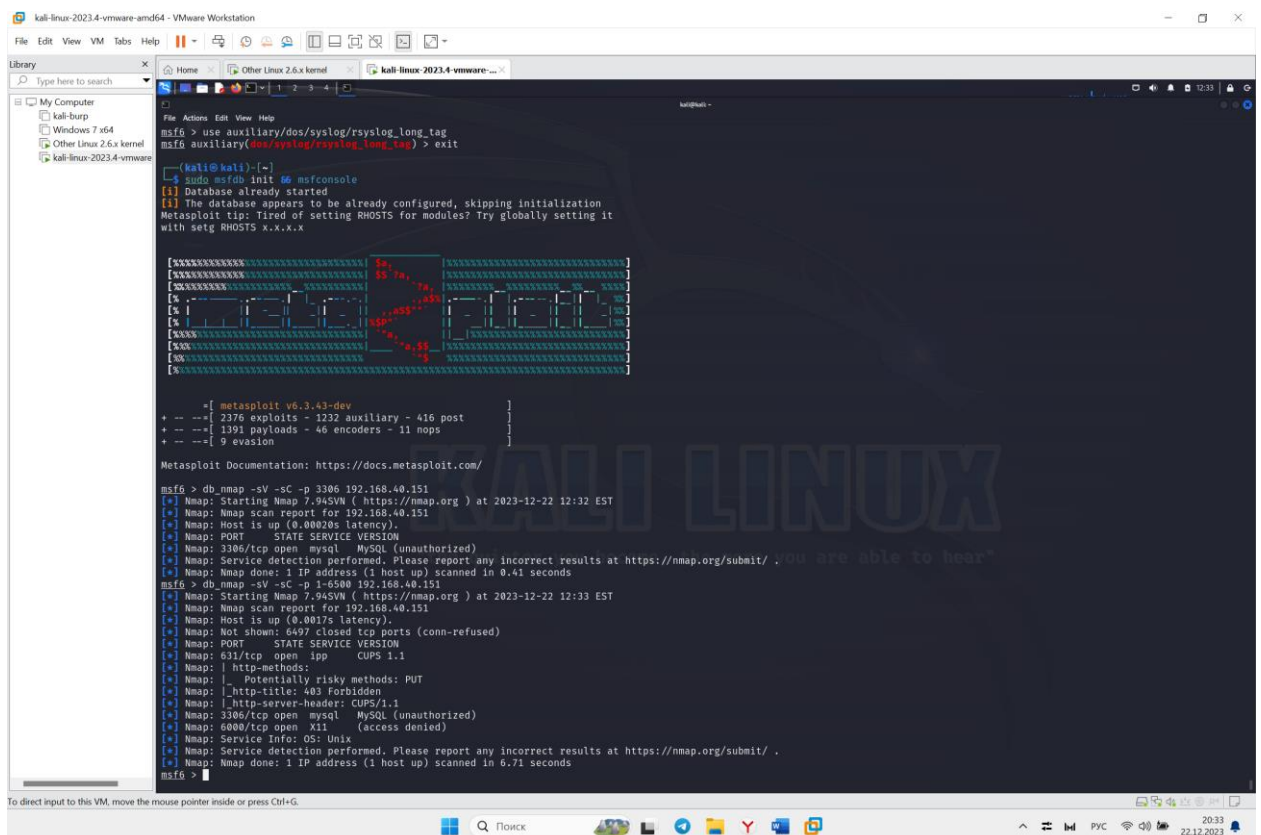
Также выполним поиск по утилите tomcat.



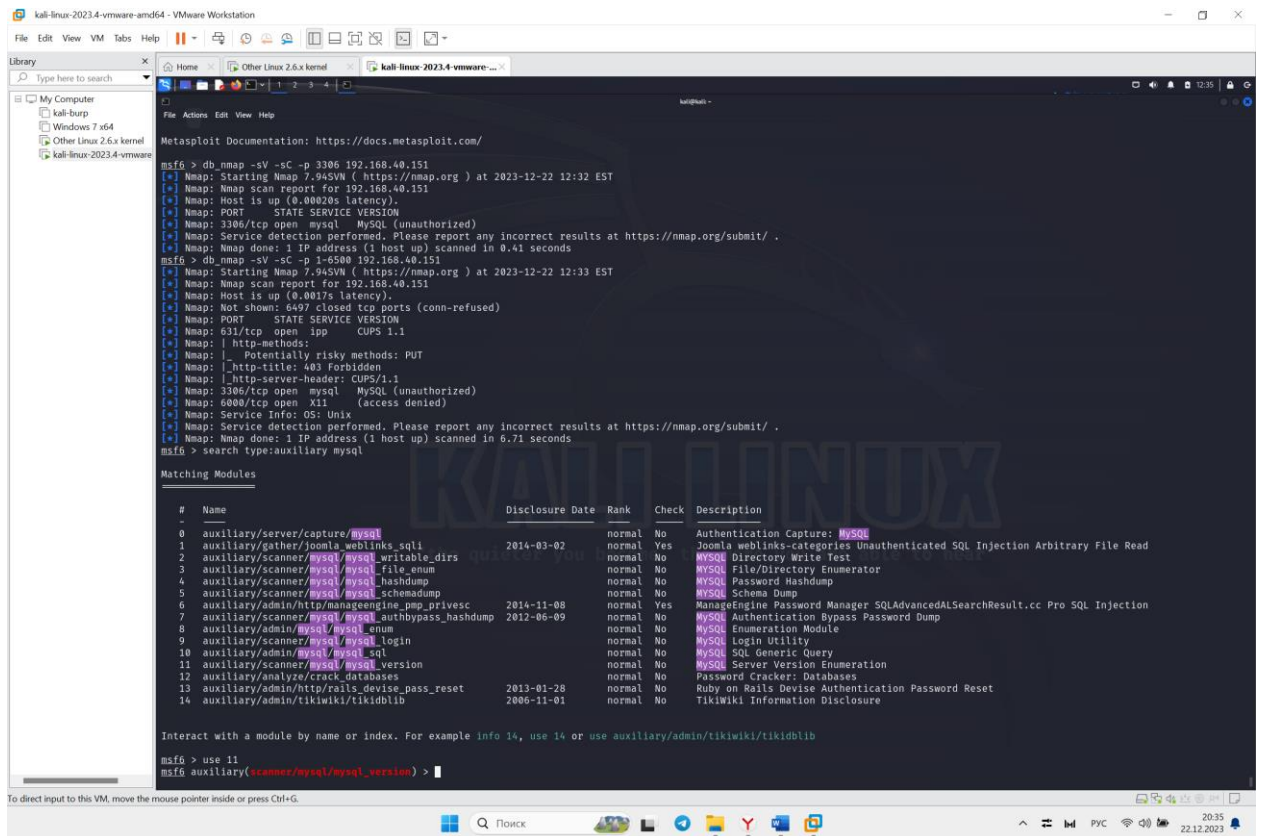
Выведем список всех доступных сканирований.



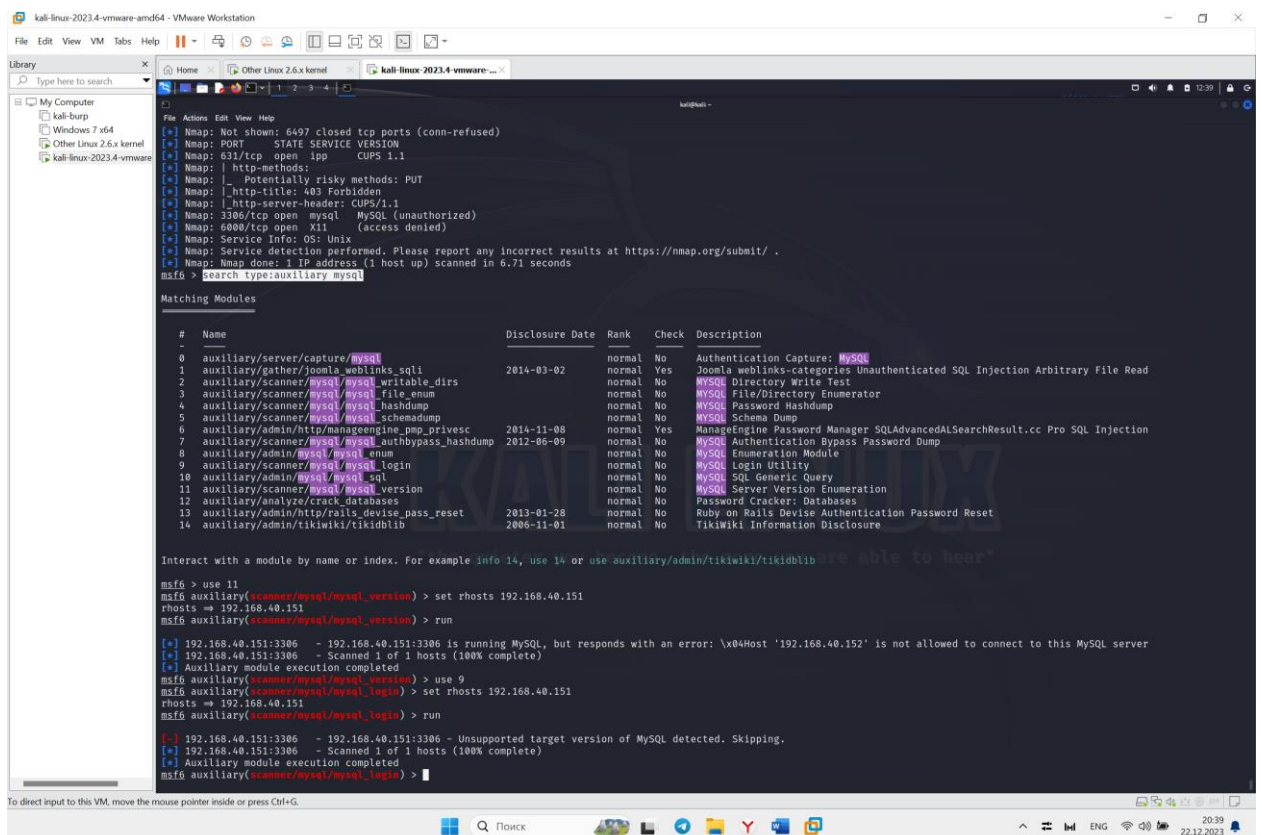
Выполним поиск эксплойтов ВМ.



Видим обнаружение MySQL. Попробуем проэсплуатировать.



Зададим необходимые параметры.



Также выполним эксплуатацию по ssh.

6. Проводите тренинги для персонала: повышайте осведомлённость о риске SQL-атак среди членов команды, отвечающей за ваше веб-приложение, и проводите ролевые тренинги для всех пользователей.
7. Контролируйте пользовательский ввод: любые пользовательские данные, указанные в SQL-запросе, несут потенциальные риски.
8. Пользуйтесь самой последней версией вашей среды разработки: в старых версиях могут отсутствовать некоторые современные функции безопасности.
9. Проводите регулярные проверки веб-приложений: пользуйтесь комплексными инструментами управления производительностью приложений, которые позволяют выявить и устранить потенциальные уязвимости до того, как они обернутся серьёзными проблемами.
10. Используйте сетевой экран веб-приложений (WAF): он фильтрует вредоносные SQL-запросы, сравнивая их с объёмными и регулярно обновляемыми списками сигнатур.