



МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

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

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Практическая работа №3.2

по дисциплине

«Управление информационной безопасностью»

Группа: ББМО-01-22, 2 курс

Выполнил: Феденёв А.В

Проверил:

Пимонов Р.В.

Москва, 2023 г.

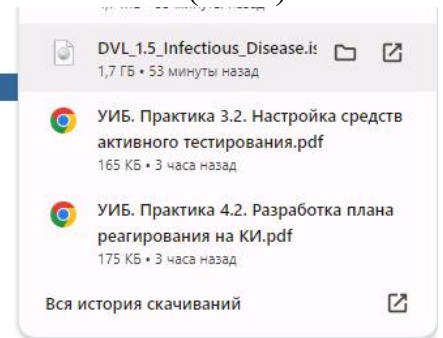
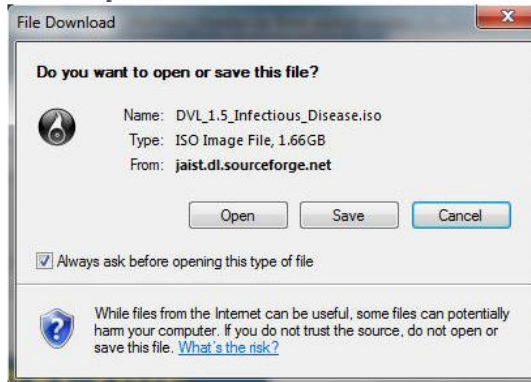
Ход работы

Установка VM (виртуальной машины) Damn Vulnerable Linux (DVL):

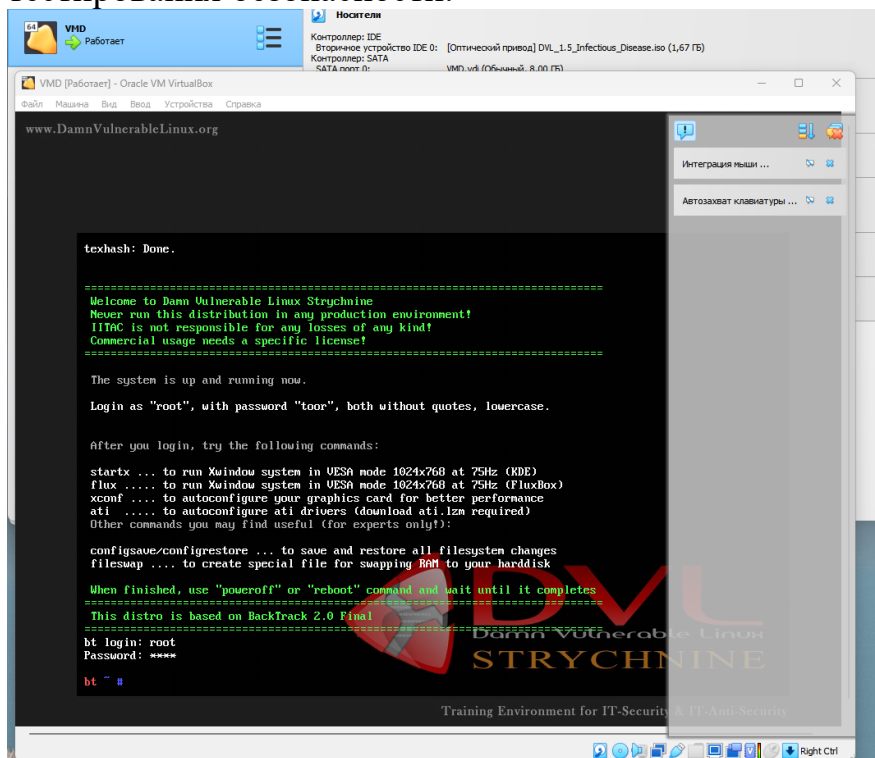
2. Загрузите iso-файл Damn Vulnerable Linux (DVL).

1. Скачать ДВЛ
 - [Кликните сюда](#)

2. Нажмите «Сохранить».

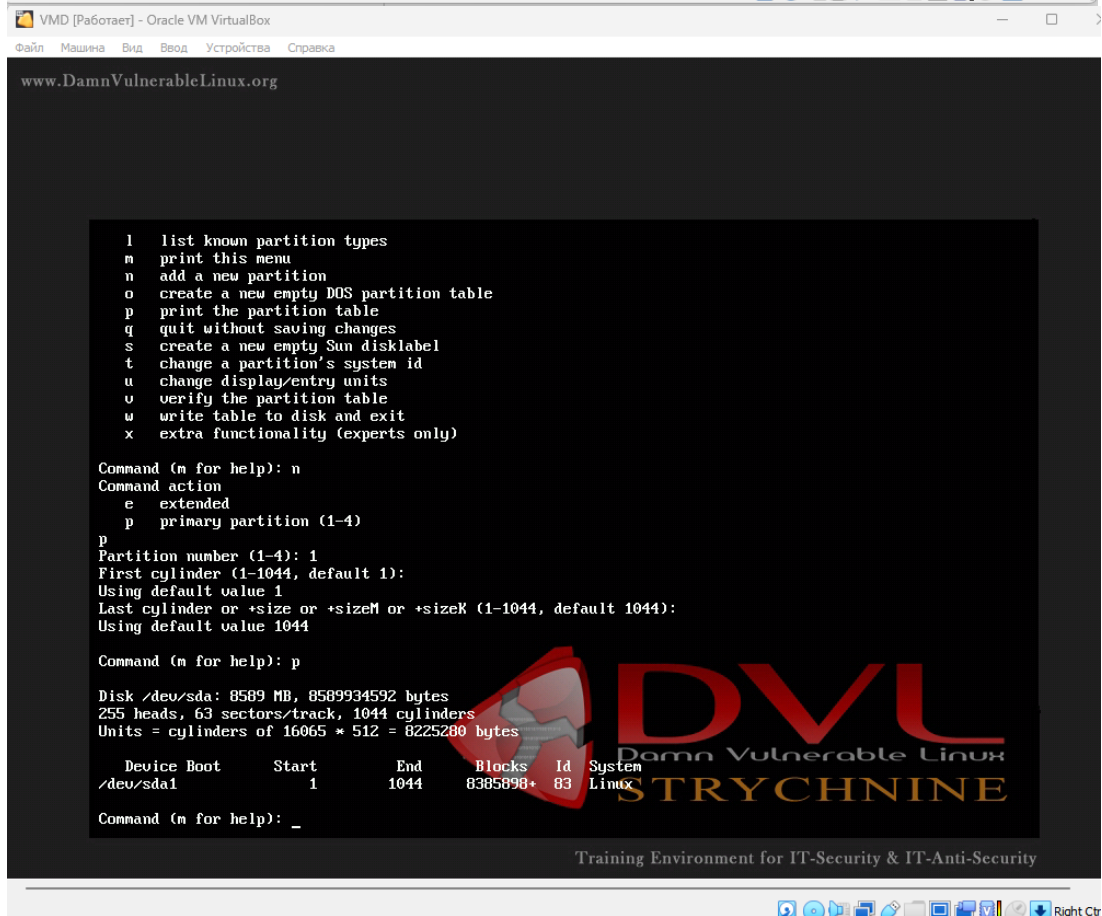
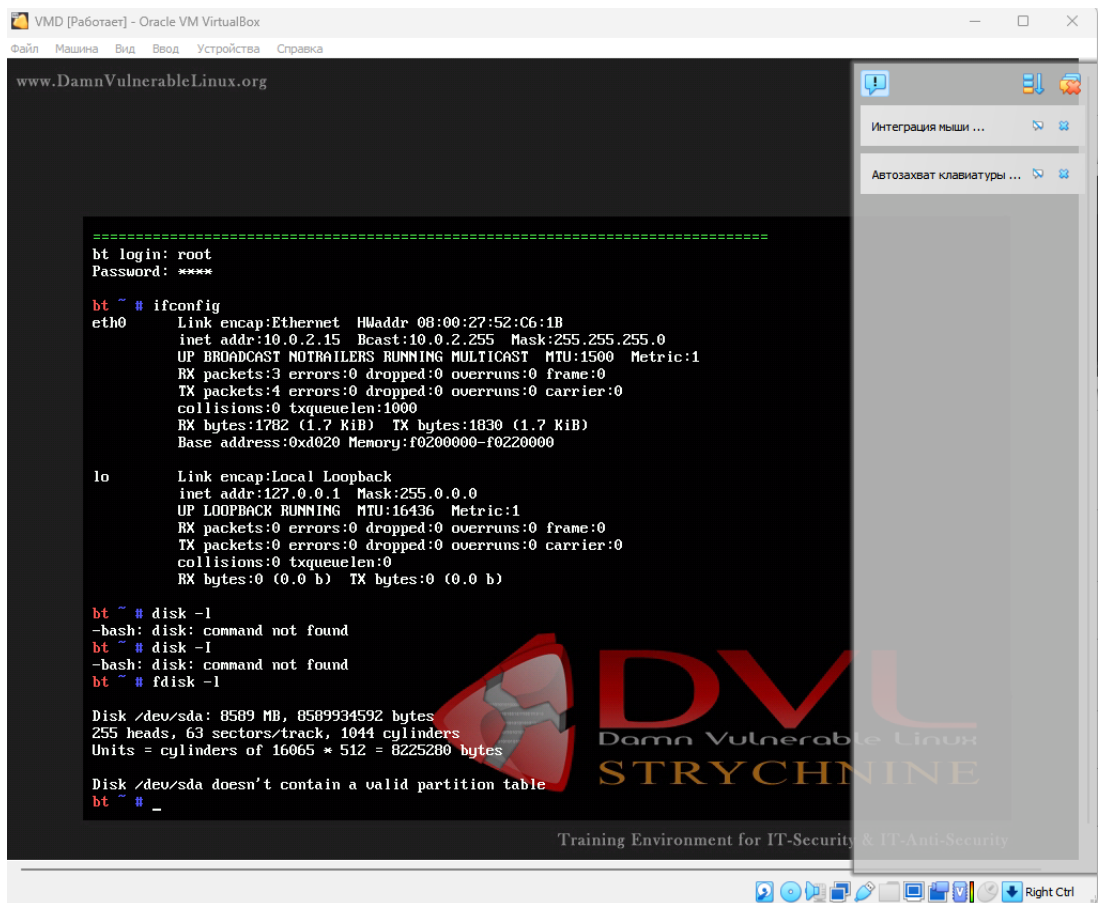


Установка DVL на отдельной виртуальной машине, настройка для тестирования безопасности.



Root; Toor

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



Форматируем диск

```

bt ~ # mkfs.ext3 /dev/sda1
mkfs 1.38 (30-Jun-2005)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
1048576 inodes, 2096474 blocks
104823 blocks (5.00%) reserved for the super user
First data block=0
64 block groups
32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 25 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
bt ~ #

```

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

Right Ctrl

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

VMD [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

www.DamnVulnerableLinux.org

```

mkfs 1.38 (30-Jun-2005)
Could not stat /dev/sda1 --- No such file or directory

The device apparently does not exist; did you specify it correctly?
bt ~ #
bt ~ # mkfs.ext3 /dev/sda1
mkfs 1.38 (30-Jun-2005)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
1048576 inodes, 2096474 blocks
104823 blocks (5.00%) reserved for the super user
First data block=0
64 block groups
32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 25 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
bt ~ # mkdir /mnt/dvl
bt ~ # mount /dev/sda1 /mnt/dvl
bt ~ # df -hT

```

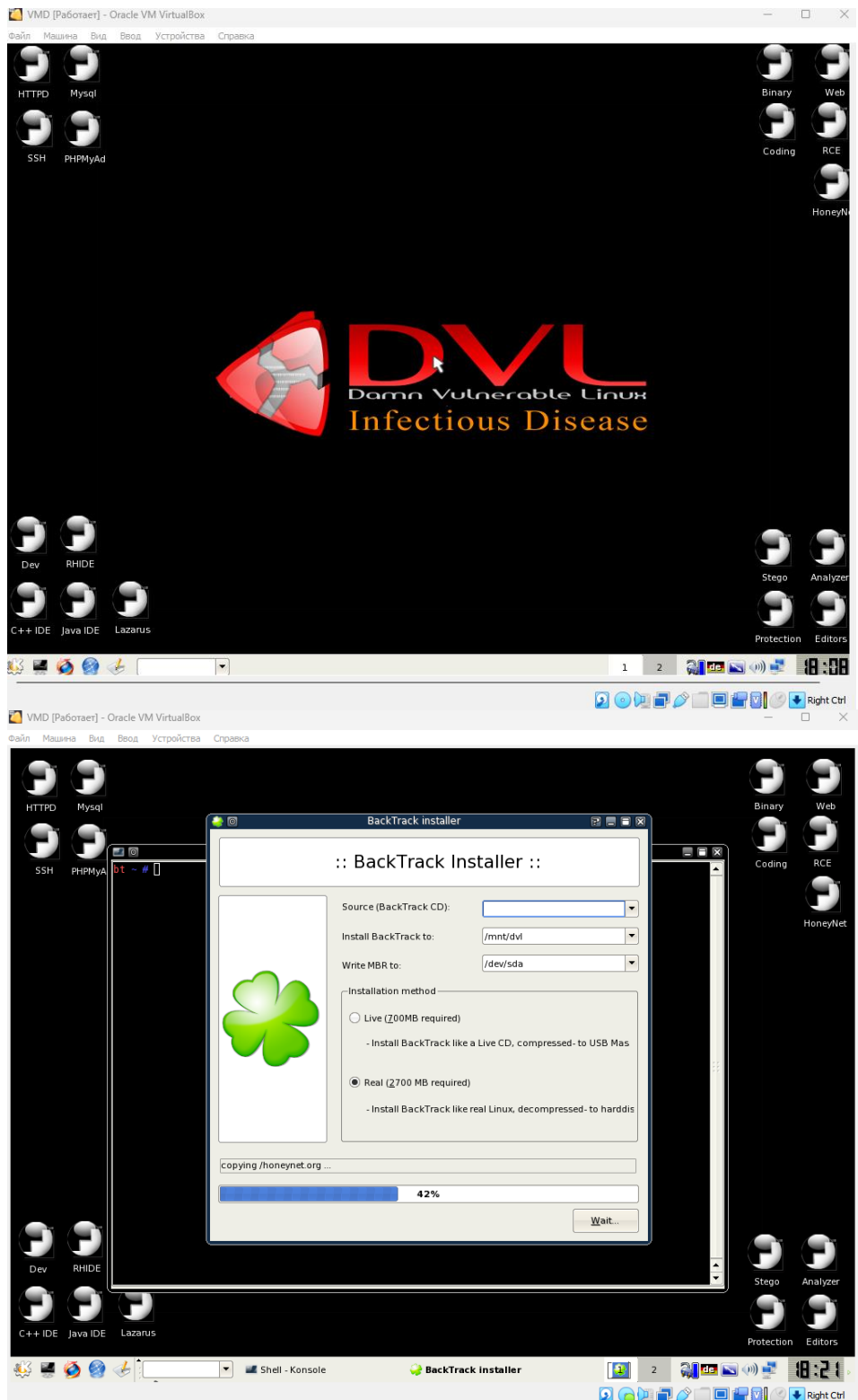
Filesystem	Type	Size	Used	Avail	Use%	Mounted on
tmpfs	tmpfs	2.1G	7.8M	2.1G	1%	/
none	tmpfs	144M	0	144M	0%	/dev/shm
/dev/sda1	ext3	7.9G	129M	7.4G	2%	/mnt/dvl

bt ~ #

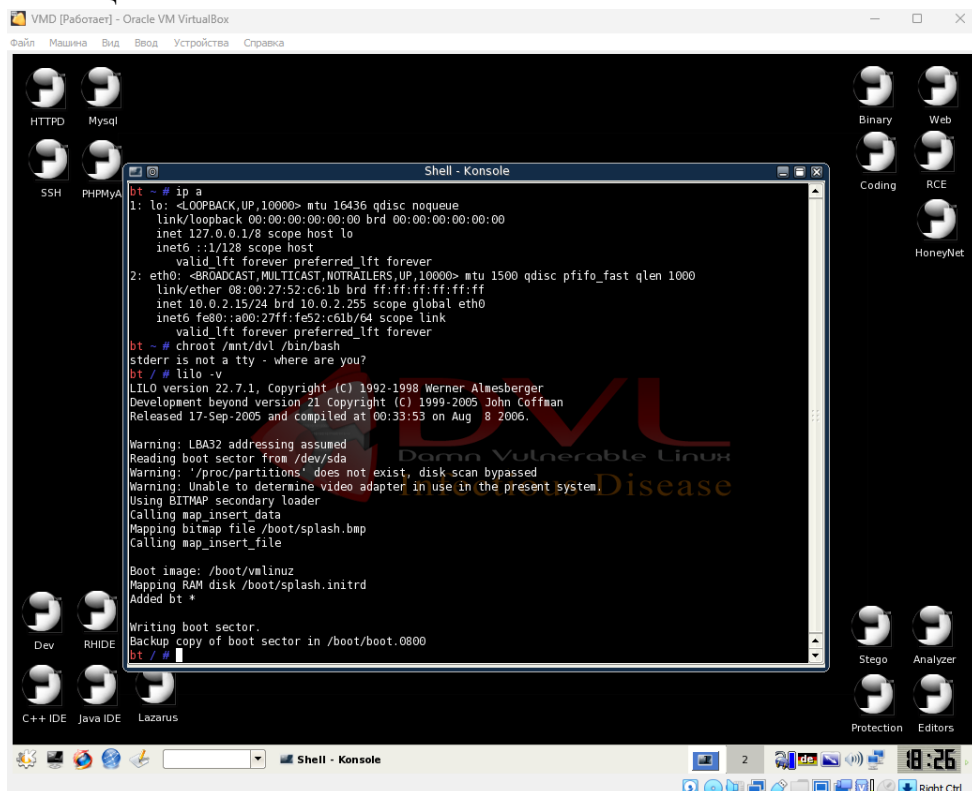
Training Environment for IT-Security & IT-Anti-Security

Right Ctrl

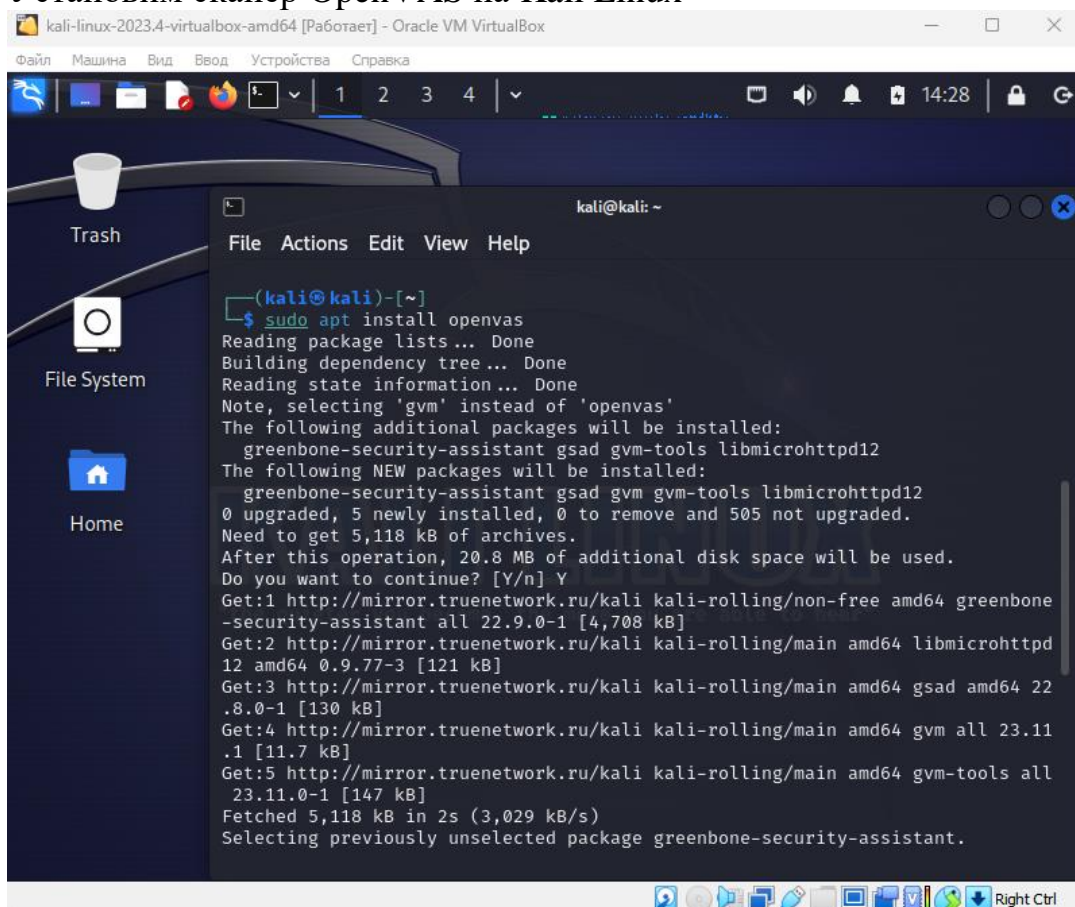
Запустим оконную систему



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



Выйдем из chroot среды и выключим VM
Установим сканер OpenVAS на Kali Linux



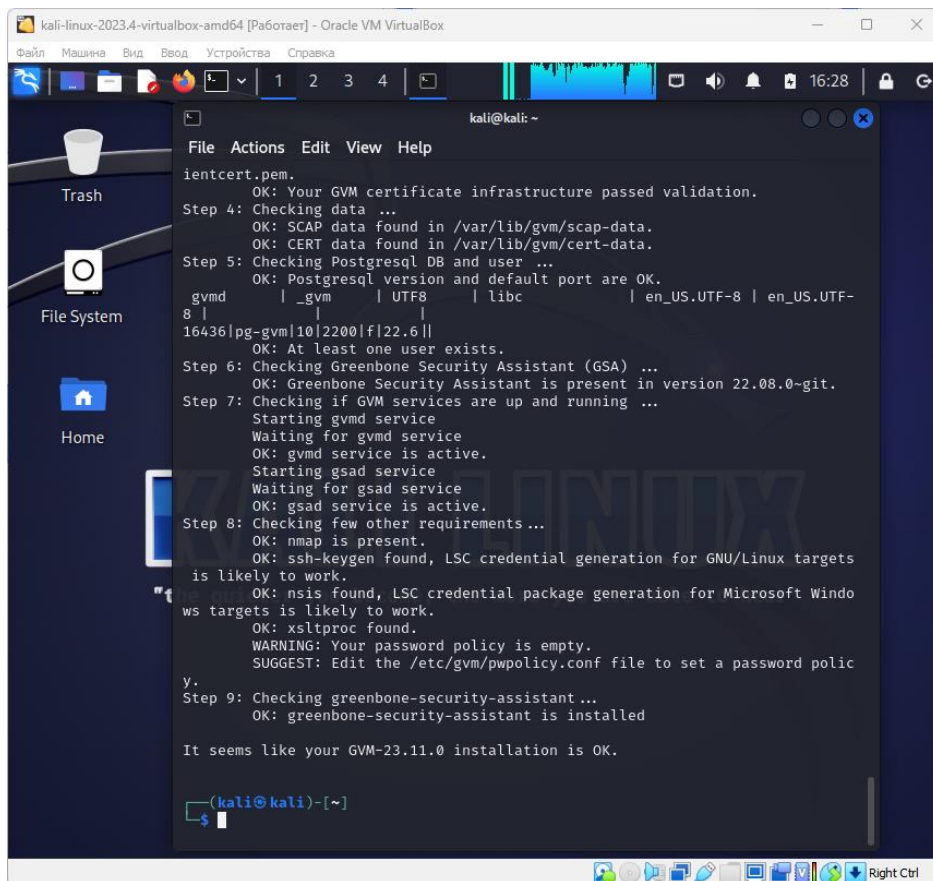
Запустим базу данных redis и включим её запуск после старта ОС

```
kali@kali: ~  
$ sudo apt install <deb name>  
  
(kali@kali)~  
$ systemctl start redis-server.service  
  
(kali@kali)~  
$ enable redis-server.service  
enable: no such hash table element: 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; pres>  
   Active: active (running) since Thu 2023-12-28 14:47:44 EST; 1min 25s ago  
     Docs: http://redis.io/documentation,  
           man:redis-server(1)  
   Main PID: 13353 (redis-server)  
   Status: "Ready to accept connections"  
    Tasks: 5 (limit: 2260)  
   Memory: 11.1M  
      CPU: 215ms  
   CGroup: /system.slice/redis-server.service  
           └─13353 /usr/bin/redis-server 127.0.0.1:6379  
  
Dec 28 14:47:44 kali systemd[1]: Starting redis-server.service - Advanced ke>  
Dec 28 14:47:44 kali systemd[1]: Started redis-server.service - Advanced key>
```

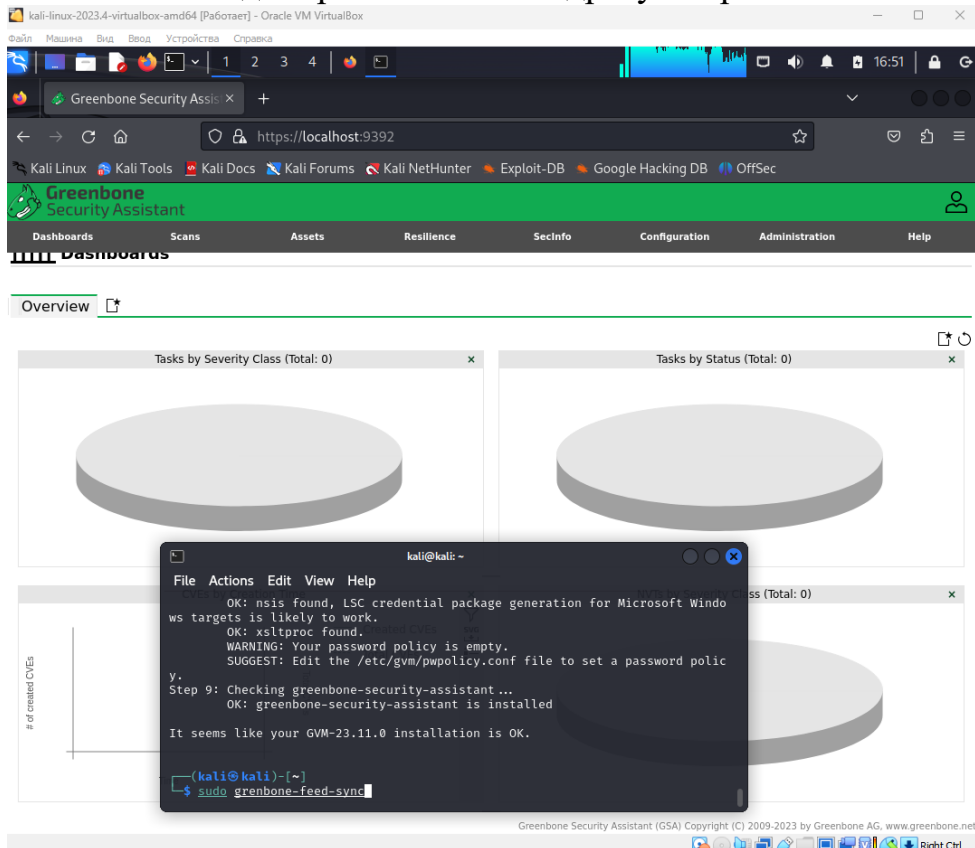
sudo gvm-setup

```
kali@kali: ~  
$ sudo gvm-setup  
[*] Creating permissions  
CREATE ROLE  
  
[*] Applying permissions  
GRANT ROLE  
  
[*] Creating extension uuid-ossdp  
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 'c444a896-ae56-4afa-b441-62164a5eb7cb'.  
[*] 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-da  
ta/notus/ to /var/lib/notus  
# Downloading NASL files from  
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-da  
ta/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
```

Проверим, что все компоненты были верно установлены и функционируют
sudo gvm-check-setup



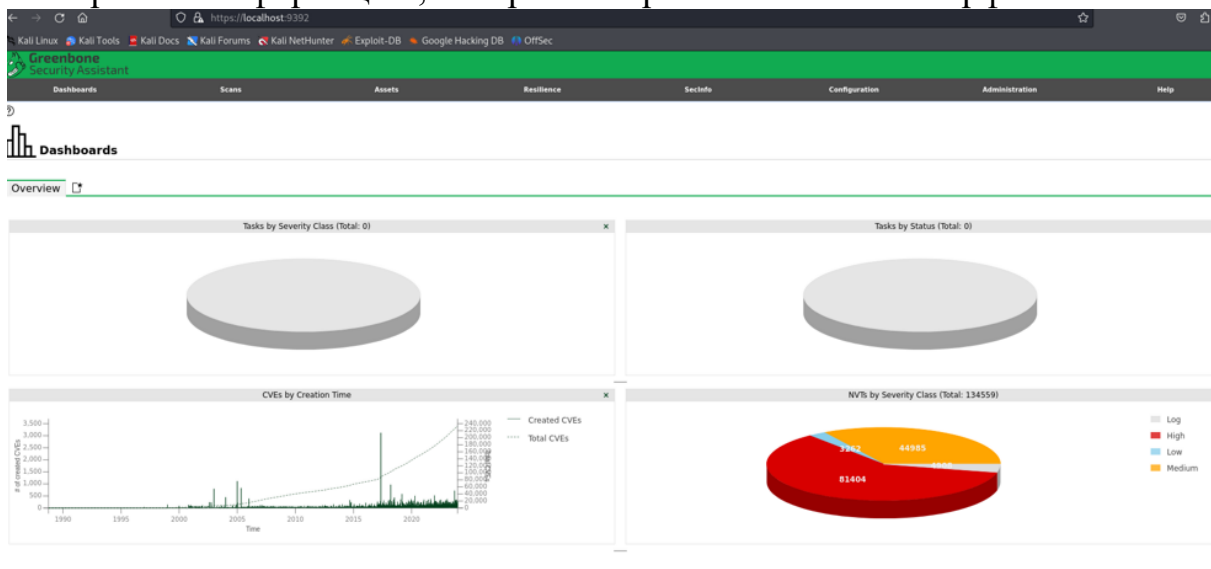
Выполним вход в приложение по адресу “https://localhost:9392”:



Обновим базы уязвимостей OpenVAS


```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo greenbone-feed-sync  
Running as root. Switching to user '_gvm' and group '_gvm'.  
Trying to acquire lock on /var/lib/opensvas/feed-update.lock  
Acquired lock on /var/lib/opensvas/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/opensvas/plugins  
Releasing lock on /var/lib/opensvas/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
```

Смотрим на информацию, которая отображается в веб-интерфейсе



Запустим сервис ssh на DVL



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

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap 10.0.2.15/24  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-29 04:27 EST  
Nmap done: 256 IP addresses (0 hosts up) scanned in 104.44 seconds  
  
(kali@kali)-[~]  
$ nmap 10.0.2.15/24  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-29 04:30 EST  
Nmap done: 256 IP addresses (0 hosts up) scanned in 104.40 seconds  
  
(kali@kali)-[~]  
$ nmap -sV --script vulners 10.0.2.15  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-29 04:32 EST  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.92 seconds  
  
(kali@kali)-[~]  
$ nmap 192.168.230.139  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-29 04:34 EST  
Nmap scan report for 192.168.230.139  
Host is up (0.0020s latency).  
Not shown: 996 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
631/tcp   open  ipp  
3306/tcp  open  mysql  
6000/tcp  open  X11  
  
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

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

```
kali@kali: ~  
File Actions Edit View Help  
  
| CVE-2009-1183 4.3 https://vulners.com/cve/CVE-2009-1183  
| CVE-2009-1181 4.3 https://vulners.com/cve/CVE-2009-1181  
| CVE-2009-0799 4.3 https://vulners.com/cve/CVE-2009-0799  
| CVE-2009-0166 4.3 https://vulners.com/cve/CVE-2009-0166  
| CVE-2009-0147 4.3 https://vulners.com/cve/CVE-2009-0147  
| CVE-2009-0146 4.3 https://vulners.com/cve/CVE-2009-0146  
| CVE-2008-5183 4.3 https://vulners.com/cve/CVE-2008-5183  
| PRION:CVE-2010-2431 2.6 https://vulners.com/prion/PRION:CVE-2010-2431  
| 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  
|_ http-server-header: CUPS/1.1  
3306/tcp open mysql MySQL (unauthorized)  
6000/tcp open X11 (access denied)  
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 7.88 seconds
```

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

Вернёмся в веб интерфейс во вкладку Scans – Tasks и укажем localhiost


```
kali@kali: ~  
File Actions Edit View Help  
17 exploit/linux/http/cisco_prime_inf_rce 2018-10-04 excellent Yes Cisco Prime I  
nfrastructure Unauthenticated Remote Code Execution  
18 post/multi/gather/tomcat_gather normal No Gather Tomcat  
Credentials  
19 auxiliary/dos/http/hashcollision_dos 2011-12-28 normal No Hashtable Col  
lisions  
20 auxiliary/admin/http/ibm_drm_download 2020-04-21 normal Yes IBM Data Risk  
Manager Arbitrary File Download  
21 exploit/linux/http/lucee_admin_imgprocess_file_write 2021-01-15 excellent Yes Lucee Adminis  
trator imgProcess.cfm Arbitrary File Write  
22 exploit/linux/http/mobileiron_core_log4shell 2021-12-12 excellent Yes MobileIron Co  
re Unauthenticated JNDI Injection RCE (via Log4Shell)  
23 exploit/multi/http/zenworks_configuration_management_upload 2015-04-07 excellent Yes Novell ZENwor  
ks Configuration Management Arbitrary File Upload  
24 exploit/multi/http/spring_framework_rce_spring4shell 2022-03-31 manual Yes Spring Framew  
ork Class property RCE (Spring4Shell)  
25 auxiliary/admin/http/tomcat_administration normal No Tomcat Admini  
stration Tool Default Access  
26 auxiliary/scanner/http/tomcat_mgr_login normal No Tomcat Applic  
ation Manager Login Utility  
27 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03 excellent Yes Tomcat RCE vi  
a JSP Upload Bypass  
28 auxiliary/admin/http/tomcat_utf8_traversal 2009-01-09 normal No Tomcat UTF-8  
Directory Traversal Vulnerability  
29 auxiliary/admin/http/trendmicro_dlp_traversal 2009-01-09 normal No TrendMicro Da  
ta Loss Prevention 5.5 Directory Traversal  
30 post/windows/gather/enum_tomcat normal No Windows Gathe  
r Apache Tomcat Enumeration  
  
Interact with a module by name or index. For example info 30, use 30 or use post/windows/gather/enum_tomcat
```

Далее поиск эксплойдов виртуальной машины

```
msf6 > db_nmap -sV -sC -p 1-65535 10.0.2.15  
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-29 04:46 EST  
[*] Nmap: Nmap scan report for 10.0.2.15  
[*] Nmap: Host is up (0.00094s latency).  
[*] Nmap: Not shown: 6496 closed tcp ports (conn-refused)  
[*] Nmap: PORT      STATE SERVICE VERSION  
[*] Nmap: 22/tcp    open  ssh      OpenSSH 4.4 (protocol 1.99)  
[*] Nmap: | ssh-hostkey:  
[*] Nmap: | 2048 dc6b00078fce5e8d55a60ae6338f0b89 (RSA1)  
[*] Nmap: | 1024 2c66a9bc421f6bb1fc572ebcb1858b59 (DSA)  
[*] Nmap: |_ 2048 0c76fe2a92e6437e5631df75f7ac93df (RSA)  
[*] Nmap: |_ sshv1: Server supports SSHv1  
[*] Nmap: 631/tcp    open ipp      CUPS 1.1  
[*] Nmap: |_ http-server-header: CUPS/1.1  
[*] Nmap: |_ http-methods:  
[*] Nmap: |_ Potentially risky methods: PUT  
[*] Nmap: |_ http-title: 403 Forbidden  
[*] Nmap: 3306/tcp    open mysql  MySQL (unauthorized)  
[*] Nmap: 6000/tcp    open X11     (access denied)  
[*] Nmap: Service Info: OS: Unix  
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/  
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 7.94 seconds
```

Выполним эксплуатацию по ssh

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/ssh/apache_karaf_command_execution	2016-02-09	normal	No	Apache Karaf Default Credentials Command Execution
1	auxiliary/scanner/ssh/karaf_login		normal	No	Apache Karaf Login Utility
2	auxiliary/scanner/ssh/cerberus_sftp_enumusers	2014-05-27	normal	No	Cerberus FTP Server SFTP Username Enumeration
3	auxiliary/dos/cisco/cisco_7937g_dos	2020-06-02	normal	No	Cisco 7937G Denial-of-Service Attack
4	auxiliary/admin/http/cisco_7937g_ssh_privilege_escalation	2020-06-02	normal	No	Cisco 7937G SSH Privilege Escalation
5	auxiliary/scanner/http/cisco_firepower_login		normal	No	Cisco Firepower Management Console 6.0 Login
6	auxiliary/scanner/ssh/eaton_xpert_backdoor	2018-07-18	normal	No	Eaton Xpert Meter SSH Private Key Exposure
7	auxiliary/scanner/ssh/fortinet_backdoor	2016-01-09	normal	No	Fortinet SSH Backdoor Scanner
8	auxiliary/scanner/http/gitlab_user_enum	2014-11-21	normal	No	GitLab User Enumeration
9	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No	Juniper SSH Backdoor Scanner
10	auxiliary/scanner/ssh/detect_kippo		normal	No	Kippo SSH Honeypot Detector
11	auxiliary/gather/qnap_lfi	2019-11-25	normal	Yes	QNAP QTS and Photo Station Local File Inclusion
12	auxiliary/fuzzers/ssh/ssh_version_15		normal	No	SSH 1.5 Version Fuzzer
13	auxiliary/fuzzers/ssh/ssh_version_2		normal	No	SSH 2.0 Version Fuzzer
14	auxiliary/fuzzers/ssh/ssh_kexinit_corrupt		normal	No	SSH Key Exchange Init Corruption
15	auxiliary/scanner/ssh/ssh_login		normal	No	SSH Login Check Scanner
16	auxiliary/scanner/ssh/ssh_identify_pubkeys		normal	No	SSH Public Key Acceptance Scanner
17	auxiliary/scanner/ssh/ssh_login_pubkey		normal	No	SSH Public Key Login Scanner
18	auxiliary/scanner/ssh/ssh_enumusers		normal	No	SSH Username Enumeration
19	auxiliary/fuzzers/ssh/ssh_version_corrupt		normal	No	SSH Version Corruption
20	auxiliary/scanner/ssh/ssh_version		normal	No	SSH Version Scanner
21	auxiliary/dos/windows/ssh/sysax_sshd_kexchange	2013-03-17	normal	No	Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
22	auxiliary/scanner/ssh/ssh_enum_git_keys		normal	No	Test SSH Github Access
23	auxiliary/scanner/ssh/libssh_auth_bypass	2018-10-16	normal	No	libssh Authentication Bypass Scanner

Сравнительный анализ

OpenVAS — это открытая система оценки уязвимости, которая используется для сканирования сетей и поиска уязвимостей в системах и

приложениях. Она предоставляет средства для выявления потенциальных угроз и уязвимостей в компьютерных системах и сетях.

Основные характеристики OpenVAS:

- Сканирование уязвимостей: OpenVAS проводит автоматическое сканирование сетей, портов и служб на наличие известных уязвимостей.
- База данных уязвимостей: Она использует обновляемую базу данных уязвимостей, чтобы определить, насколько системы уязвимы к известным атакам.
- Отчеты и анализ: OpenVAS генерирует отчеты о найденных уязвимостях и предоставляет анализ безопасности сети.

Nmap — это мощное средство сканирования сети, которое используется для анализа и исследования сетей, определения активных хостов, портов и служб, а также выявления уязвимостей.

Основные характеристики Nmap:

- Сканирование сети: Nmap позволяет сканировать сети для поиска активных хостов, открытых портов и служб, работающих на этих портах.
- Определение уязвимостей: с помощью дополнительных сценариев и плагинов Nmap может выявлять уязвимости и выполнять сканирование на наличие известных уязвимостей.
- Скрипты и пользовательские сценарии: Nmap поддерживает создание собственных скриптов и сценариев для выполнения специфических задач.

Сходства:

1. Сканирование сети: как OpenVAS, так и Nmap предназначены для сканирования сети и выявления уязвимостей.
2. Базы данных уязвимостей: Обе системы могут использовать базы данных уязвимостей для определения уровня уязвимости систем.
3. Отчеты: как OpenVAS, так и Nmap способны генерировать отчеты о результатах сканирования.

Различия:

1. Цель использования:

OpenVAS прежде всего ориентирован на сканирование уязвимостей и проведение анализа безопасности.

Nmap, хотя также может выполнять сканирование уязвимостей, в первую очередь используется для сбора информации о сетях и хостах.

2. Функциональность:

OpenVAS более специализирован для оценки уязвимостей и имеет расширенные инструменты для этой цели.

Nmap имеет более широкий набор функций, включая определение активных хостов, сбор информации о службах и портах.

3. Интерфейс пользователя:

OpenVAS: OpenVAS обычно имеет веб-интерфейс, который удобен для настройки и управления задачами сканирования. Он также предоставляет отчеты в удобном виде для анализа результатов.

Nmap: Nmap в основном используется через командную строку, но также имеет графические оболочки для удобства пользователей. Он обычно предоставляет текстовые результаты сканирования.

4. Сценарии и расширения:

OpenVAS: OpenVAS предоставляет сценарии и плагины, которые позволяют пользователю выполнять дополнительные проверки безопасности и анализировать уязвимости на более глубоком уровне.

Nmap: Nmap также позволяет пользователю создавать пользовательские сценарии и расширения, но его основной фокус — это сбор базовой информации о сети.

5. Подход к безопасности:

OpenVAS: OpenVAS более ориентирован на более высокий уровень безопасности и предназначен для выявления и решения уязвимостей в системах.

Nmap: Nmap, хотя и может выполнять сканирование уязвимостей, более фокусируется на сборе информации о сети и не обязательно на выявлении уязвимостей.

Заключение

OpenVAS: OpenVAS подходит для оценки безопасности информационных систем, сетей и приложений. Его можно использовать в корпоративных средах и организациях, чтобы регулярно проверять и обнаруживать уязвимости в сетях и серверах.

Nmap: Nmap может быть полезным инструментом для администраторов сетей и безопасности, когда требуется получить информацию о сетевой инфраструктуре, определить активные хосты, контролировать открытые порты и проводить исследование сетей. Он также может использоваться для сканирования уязвимостей, но его главное предназначение — это сбор информации о сети.