



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

---

**Институт кибербезопасности и цифровых технологий**  
**Практическая работа № 3.2**  
**по дисциплине**  
**«Управление информационной безопасностью»**

**Выполнил:**

**ББМО–01–22**

**Чадов В. Т.**

**Проверил:**

**Пимонов Р. В.**

**«Зачтено»**

**«\_\_»\_\_\_\_\_2023 г. \_\_\_\_\_**

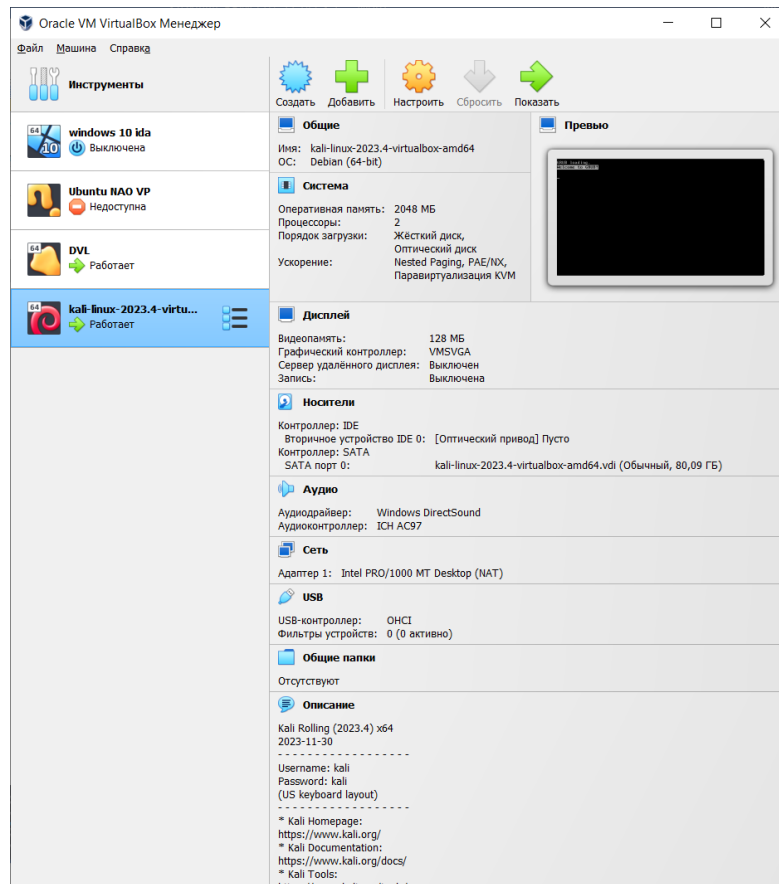
**Москва 2023**

## Содержание

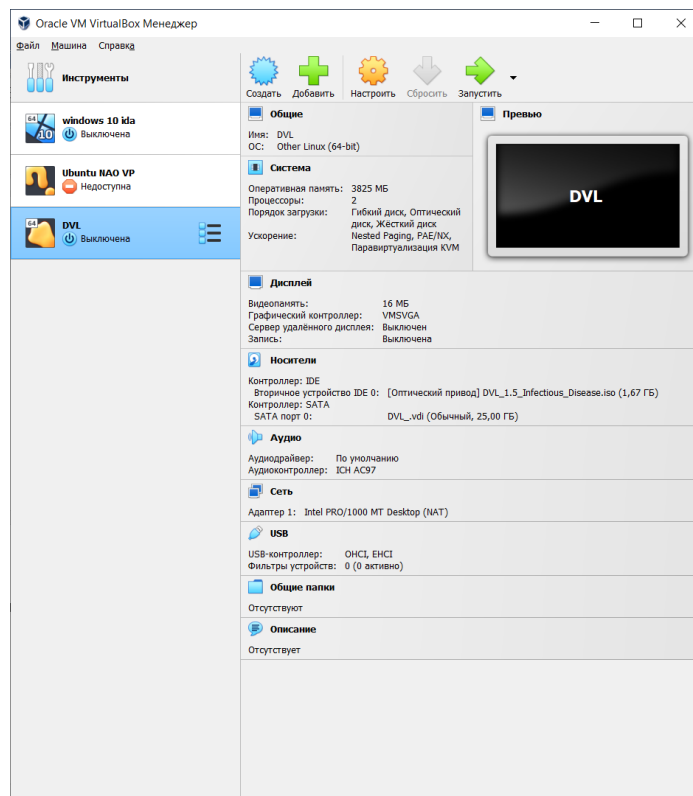
Установка и настройка виртуальных машин .....	3
Использование инструментов анализа защищенности .....	14
Анализ полученных результатов .....	21

# Установка и настройка виртуальных машин

## Добавим и запустим Kali linux



## Создадим вм с DamnVulnerableLinux



Установим все необходимое для dvl. Используя tutorial для настройки [https://www.computersecuritystudent.com/SECURITY\\_TOOLS/DVL/lesson1/](https://www.computersecuritystudent.com/SECURITY_TOOLS/DVL/lesson1/).

Требуется авторизация root/toor

```
www.DamnVulnerableLinux.org

texhash: Updating /usr/share/texmf/ls-R...
texhash: Updating /usr/share/texmf-var/ls-R...
texhash: Updating /var/tmp/tex/fonts/ls-R...
texhash: Done.

=====
Welcome to Damn Vulnerable Linux Strychnine
Never run this distribution in any production environment!
IITAC is not responsible for any losses of any kind!
Commercial usage needs a specific license!
=====

The system is up and running now.

Login as "root", with password "toor", both without quotes, lowercase.

After you login, try the following commands:

startx ... to run Xwindow system in VESA mode 1024x768 at 75Hz (KDE)
flux .... to run Xwindow system in VESA mode 1024x768 at 75Hz (FluxBox)
xconf .... to autoconfigure your graphics card for better performance
ati .... to autoconfigure ati drivers (download ati.lzm required)
Other commands you may find useful (for experts only!):

configsave/configrestore ... to save and restore all filesystem changes
fileswap .... to create special file for swapping RAM to your harddisk

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

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

```
www.DamnVulnerableLinux.org

=====
Welcome to Damn Vulnerable Linux Strychnine
Never run this distribution in any production environment!
IITAC is not responsible for any losses of any kind!
Commercial usage needs a specific license!
=====

The system is up and running now.

Login as "root", with password "toor", both without quotes, lowercase.

After you login, try the following commands:

startx ... to run Xwindow system in VESA mode 1024x768 at 75Hz (KDE)
flux .... to run Xwindow system in VESA mode 1024x768 at 75Hz (FluxBox)
xconf .... to autoconfigure your graphics card for better performance
ati .... to autoconfigure ati drivers (download ati.lzm required)
Other commands you may find useful (for experts only!):

configsave/configrestore ... to save and restore all filesystem changes
fileswap .... to create special file for swapping RAM to your harddisk

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 ~ # ls
Desktop/  Set\ IP\ address  argo.user.properties  liboars.h  gen\  workSpace/
QEMU     WebScarab.properties  argounl.log           lida/     sample_scripts

bt ~ # _

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

## Проверим что у вл есть доступ к сети и друг другу

```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::5011:70bc:4a8a:81c7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:11:00 txqueuelen 1000 (Ethernet)
    RX packets 15 bytes 10688 (10.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27 bytes 4838 (4.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::89b7:2fa1:d774:d8e5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:3b:81:59 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 590 (590.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 2867 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.53 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=2.54 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=2.85 ms
^C
--- 192.168.56.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2023ms
rtt min/avg/max/ndev = 1.525/2.038/2.535/0.412 ms

kali@kali:~$
```

```
www.DamnVulnerableLinux.org

*****
This distro is based on BackTrack 2.0 Final
*****
bt login: root
Password: ****

bt ~ # ifconfig
eth0    Link encap:Ethernet  HWaddr 08:00:27:2F:6F:8F
        inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
        UP BROADCAST MULTICAST  RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:13 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:4820 (4.7 KiB)  TX bytes:1830 (1.7 KiB)
        Base address:0xd020  Memory:102000000-102200000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:65536  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 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data:
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.837 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.820 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=1.32 ms
^C
--- 192.168.56.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/ndev = 0.837/1.016/1.323/0.220 ms

bt ~ #
```

Настроим DVL, выведем `fdisk -l` и видим отсутствие таблицы разделов, создадим новую

```
bt ~ # fdisk -l

Disk /dev/sda: 22.2 GB, 2283698176 bytes
255 heads, 63 sectors/track, 2709 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Disk /dev/sda doesn't contain a valid partition table
```

```
bt ~ # fdisk /dev/sda
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previous
content won't be recoverable.
```

```
Command (m for help): m
Command action
a   toggle a bootable flag
b   edit bsd disklabel
c   toggle the dos compatibility flag
d   delete a partition
l   list known partition types
m   print this menu
n   add a new partition
o   create a new empty DOS partition table
p   print the partition table
q   quit without saving changes
s   create a new empty Sun disklabel
t   change a partition's system id
u   change display/entry units
v   verify the partition table
w   write table to disk and exit
x   extra functionality (experts only)
```

```

Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
1
Invalid partition number for type `1'
Command action
  e   extended
  p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-2709, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-2709, default 2709):
Using default value 2709

```

Видим новую таблицу разделов

```

bt ~ # fdisk -l

Disk /dev/sda: 22.2 GB, 22283698176 bytes
255 heads, 63 sectors/track, 2709 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1             1         2709     21760011   83   Linux

```

Отформатируем диск

```

bt ~ # mkfs.ext3 /dev/sda1
mke2fs 1.38 (30-Jun-2005)
warning: 514 blocks unused.

Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
2725056 inodes, 5439488 blocks
272000 blocks (5.00%) reserved for the super user
First data block=0
166 block groups
32768 blocks per group, 32768 fragments per group
16416 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000

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

This filesystem will be automatically checked every 28 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.

```

Создадим директорию /mnt/dv1 и примонтируем туда созданный раздел /dev/sda1

```

bt ~ # mkdir /mnt/dv1
bt ~ # mount /dev/sda1 /mnt/dv1
bt ~ # df -hT

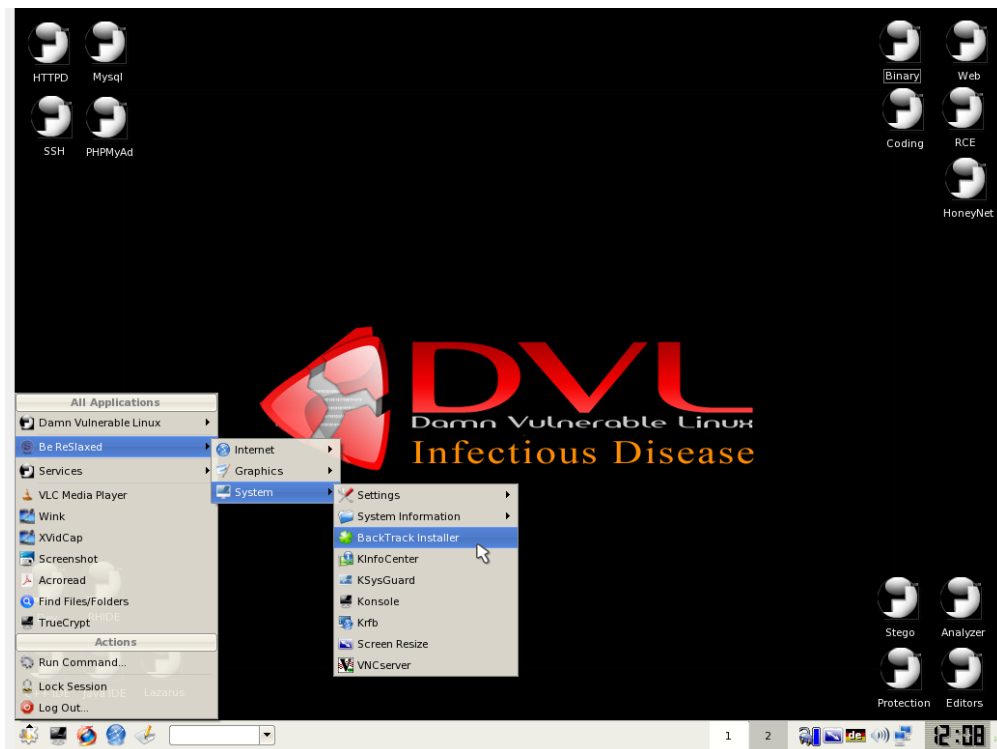
```

Filesystem	Type	Size	Used	Avail	Use%	Mounted on
tmpfs	tmpfs	1.8G	7.8M	1.8G	1%	/
none	tmpfs	144M	0	144M	0%	/dev/shm
/dev/sda1	ext3	21G	129M	20G	1%	/mnt/dv1

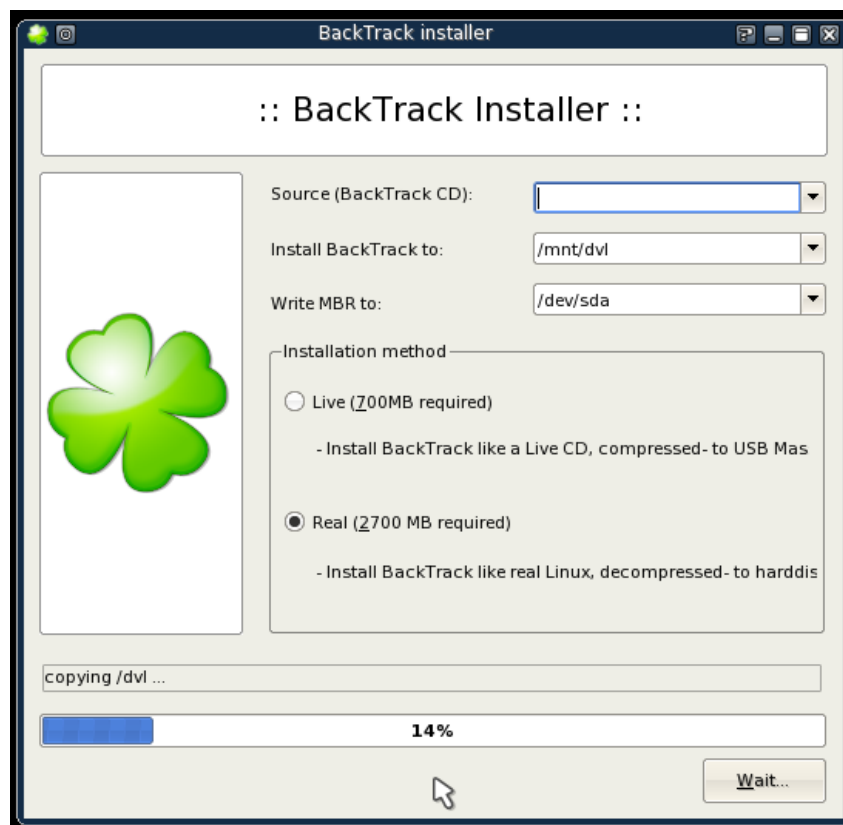
Запустим графическую оболочку

```
bt ~ # startx & _
```

Запустим BackTrack Installer



Установим с параметрами как на картинке



Также подправим сломавшуюся раскладку клавиатуры только на US





## Установим boot loader при помощи lilo


```
Shell - Konsole
bt ~ # chroot /mnt/dvl /bin/bash
stderr is not a tty - where are you?
bt / # lilo -v
LILO version 22.7.1, Copyright (C) 1992-1998 Werner Almesberger
Development beyond version 21 Copyright (C) 1999-2005 John Coffman
Released 17-Sep-2005 and compiled at 00:33:53 on Aug  8 2006.

Warning: LBA32 addressing assumed
Reading boot sector from /dev/sda
Warning: '/proc/partitions' does not exist, disk scan bypassed
Warning: Unable to determine video adapter in use in the present system.
Using BITMAP secondary loader
Calling map_insert_data
Mapping bitmap file /boot/splash.bmp
Calling map_insert_file

Boot image: /boot/vmlinuz
Mapping RAM disk /boot/splash.initrd
Added bt *

Writing boot sector.
Backup copy of boot sector in /boot/boot.0800
bt / #
```

## Перезапустим вм и отключим iso файл

 **Носители**

Контроллер: IDE  
Вторичное устройство IDE 0: [Оптический привод] Пусто  
Контроллер: SATA  
SATA порт 0: DVL.vdi (Обычный, 20,75 ГБ)

## Повторно проверим соединение и подключение к интернету

kali@kali: ~  
File Actions Edit View Help  
ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255  
inet6 fe80::501:70bc:6a8:31c7 prefixlen 64 scopeid 0<20clink>  
ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)  
RX packets 15 bytes 10688 (10.4 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 27 bytes 8838 (8.6 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet6 fe80::89b7:2fal:d74:dbes prefixlen 64 scopeid 0<20clink>  
ether 08:00:27:2b:01:59 txqueuelen 1000 (Ethernet)  
RX packets 1 bytes 590 (590 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 16 bytes 2867 (2.7 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0<10<host>  
loop txqueuelen 1000 (local loopback)  
RX packets 4 bytes 240 (240 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 4 bytes 240 (240 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
[kali@kali:~]-  
\$ ping 192.168.56.101  
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:  
64 bytes from 192.168.56.101: icmp\_seq=1 ttl=64 time=1.53 ms  
64 bytes from 192.168.56.101: icmp\_seq=2 ttl=64 time=2.54 ms  
64 bytes from 192.168.56.101: icmp\_seq=3 ttl=64 time=2.05 ms  
^C  
--- 192.168.56.101 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2023ms  
rtt min/avg/max/ndev = 1.525/2.038/2.535/0.412 ms  
  
[kali@kali:~]-  
\$ ping 192.168.56.101  
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:  
64 bytes from 192.168.56.101: icmp\_seq=1 ttl=64 time=4.93 ms  
64 bytes from 192.168.56.101: icmp\_seq=2 ttl=64 time=1.73 ms  
^C  
--- 192.168.56.101 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/ndev = 1.732/3.329/4.927/1.597 ms  
  
[kali@kali:~]-  
\$

Shell - Konsole  
Base address: 0xd020 Memory: f0200000-f0200000  
  
eth2 Link encap: Ethernet Header 08:00:27:81:67:63  
inet addr: 10.0.4.15 Bcast: 10.0.4.255 Mask: 255.255.255.0  
inet6 addr: fe80::a00:27ff:fe01:6303/64 ScopeLink  
UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU: 1500 Metric: 1  
RX packets: 2 errors: 0 dropped: 0 overruns: 0 frame: 0  
TX packets: 9 errors: 0 dropped: 0 overruns: 0 carrier: 0  
collisions: 0 txqueuelen: 1000  
RX bytes: 1188 (1.1 KiB) TX bytes: 1708 (1.6 KiB)  
Base address: 0xd048 Memory: f0400000-f0400000  
  
lo Link encap: Local Loopback  
inet addr: 127.0.0.1 Mask: 255.0.0.0  
inet6 addr: ::1/128 Scope: Host  
UP LOOPBACK RUNNING MTU: 16384 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 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:  
64 bytes from 8.8.8.8: icmp\_seq=1 ttl=62 time=23.5 ms  
64 bytes from 8.8.8.8: icmp\_seq=2 ttl=62 time=20.7 ms  
^C  
--- 8.8.8.8 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1000ms  
rtt min/avg/max/ndev = 20.729/22.161/23.593/1.432 ms  
bt - # ping 192.168.56.101  
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:  
64 bytes from 192.168.56.101: icmp\_seq=1 ttl=64 time=1.09 ms  
64 bytes from 192.168.56.101: icmp\_seq=2 ttl=64 time=1.25 ms  
^C  
--- 192.168.56.101 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 999ms  
rtt min/avg/max/ndev = 1.093/1.175/1.257/0.082 ms  
bt - #

## Установим openvas для kali linux

```
sudo apt update
sudo apt upgrade -y
sudo apt dist-upgrade -y
sudo apt install openvas
```

```
(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 /usr/lib/systemd/systemd-sysv-installer.
Executing: /usr/lib/systemd/systemd-sysv-install enable redis-server
Failed to enable unit: Access denied

(kali㉿kali)-[~]
└─$ sudo systemctl enable redis-server.service
Synchronizing state of redis-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-installer.
Executing: /usr/lib/systemd/systemd-sysv-install enable redis-server
Created symlink /etc/systemd/system/redis.service → /usr/lib/systemd/system/redis-server.service.
Created symlink /etc/systemd/system/multi-user.target.wants/redis-server.service → /usr/lib/systemd/system/redis-server.service.

(kali㉿kali)-[~]
└─$ sudo systemctl status redis-server.service
● redis-server.service - Advanced key-value store
   Loaded: loaded (/usr/lib/systemd/system/redis-server.service; enabled; preset: disabled)
   Active: active (running) since Tue 2024-01-23 07:57:42 EST; 36s ago
     Docs: http://redis.io/documentation,
           man:redis-server(1)
  Main PID: 61878 (redis-server)
    Status: "Ready to accept connections"
     Tasks: 5 (limit: 2260)
    Memory: 11.3M (peak: 11.8M)
       CPU: 100ms
    CGroup: /system.slice/redis-server.service
            └─61878 "/usr/bin/redis-server 127.0.0.1:6379"

Jan 23 07:57:42 kali systemd[1]: Starting redis-server.service - Advanced key-value store...
Jan 23 07:57:42 kali systemd[1]: Started redis-server.service - Advanced key-value store.
```

```

(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-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 'c63797dc-dee1-4408-a572-a18ed871315f'.
[*] 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
F Downloading Notus files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ to /var/lib/notus

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

[+] Done
[*] Please note the password for the admin user
[*] User created with password 'c63797dc-dee1-4408-a572-a18ed871315f'.

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

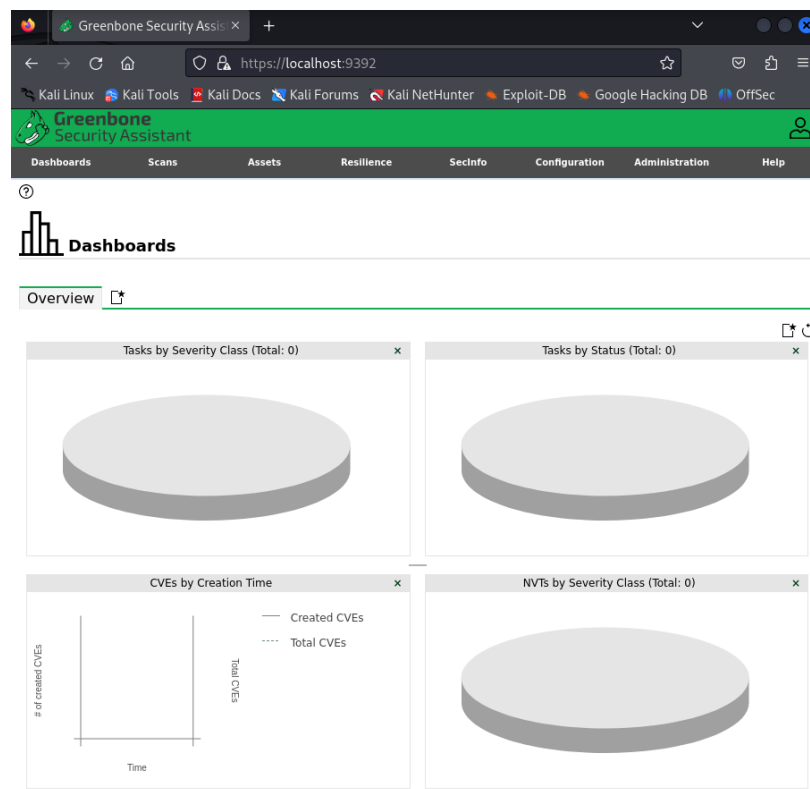
```

c63797dc-dee1-4408-a572-a18ed871315f

## Проверим корректность установки

```
(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 22.7.9.
  OK: Notus Scanner 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_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 88018 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 such 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 GVMD Manager ...
  OK: GVM Manager (gvmd) is present in version 23.1.0.
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: CERT data found in /var/lib/gvm/cert-data.
Step 5: Checking PostgreSQL DB and user ...
  OK: PostgreSQL version and default port are OK.
  gvmd | _gvm | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | |
  16436|pg-gvm|10|2200|f|22.6||
  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 gvmd service
Waiting for gvmd service
```

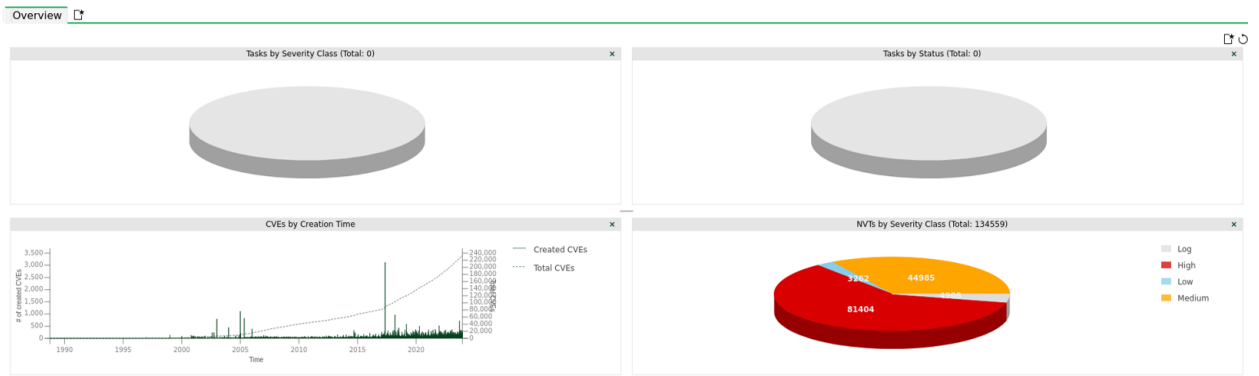
## Войдем в интерфейс приложения



## Обновим базы данных openvas

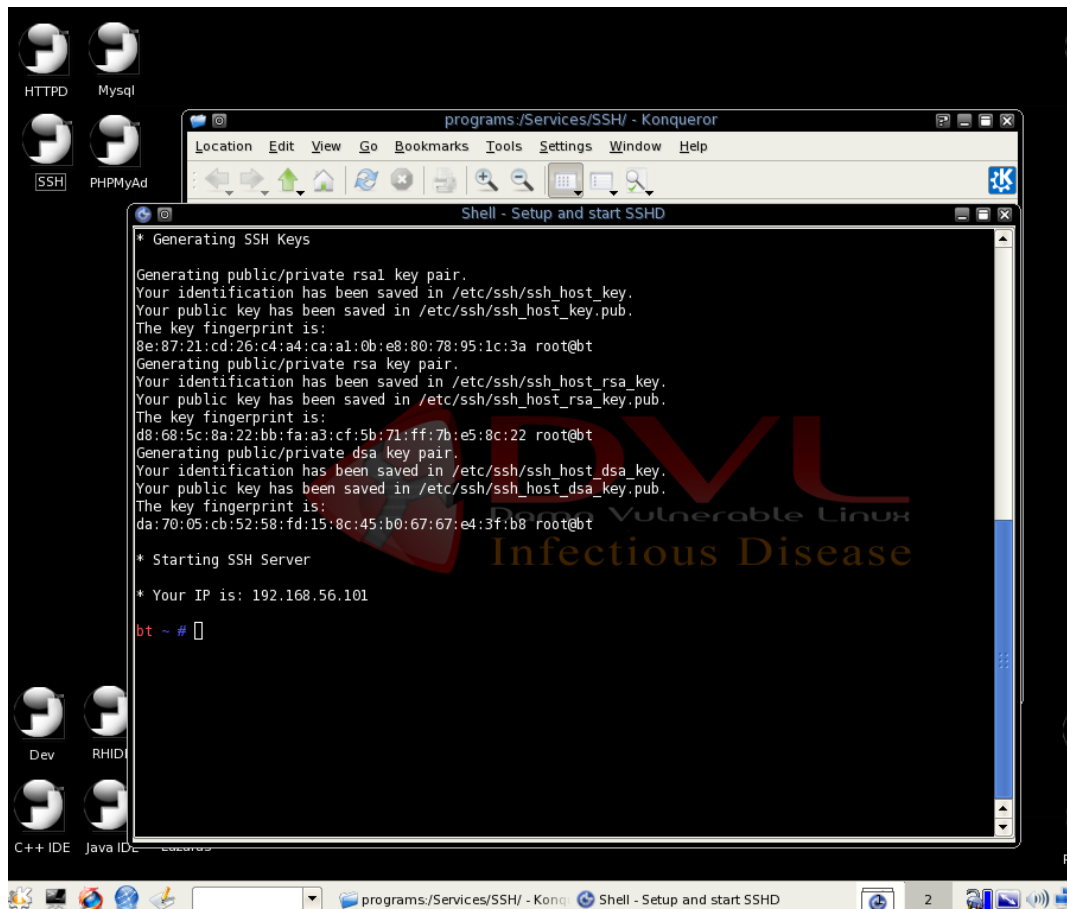
```
(kali@kali)-[~]
└─$ sudo greenbone-feed-sync
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
! Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ 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
```



# Использование инструментов анализа защищенности

Запустим ssh server на dvl



Просканируем dvl через nmap, видим открытые порты

```
(kali@kali)-[~]
$ nmap 192.168.56.101/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 09:22 EST
Nmap scan report for 192.168.56.101
Host is up (0.00043s 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 scan report for 192.168.56.102
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (2 hosts up) scanned in 19.88 seconds
```



## Просканируем при помощи скрипта vulners, уязвимости найденные nmap

```
(kali@kali)-[~]
$ nmap -sV --script vulners 192.168.56.101/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 09:24 EST
Nmap scan report for 192.168.56.101
Host is up (0.0020s latency).
Not shown: 996 closed tcp ports (conn-refused)
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
|   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
|   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
```

```

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:B5
E7D30E7583980F37EF6DBC0B05FBC3 *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
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 ip 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
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

```



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	
SSV:4583	4.3	https://vulners.com/seebug/SSV:4583	*EXPLOIT*
SSV:19826	4.3	https://vulners.com/seebug/SSV:19826	*EXPLOIT*
PRION:CVE-2014-2856	4.3	https://vulners.com/prion/PRION:CVE-2014-2856	
PRION:CVE-2010-1748	4.3	https://vulners.com/prion/PRION:CVE-2010-1748	
PRION:CVE-2009-1183	4.3	https://vulners.com/prion/PRION:CVE-2009-1183	
PRION:CVE-2009-1181	4.3	https://vulners.com/prion/PRION:CVE-2009-1181	
PRION:CVE-2009-0799	4.3	https://vulners.com/prion/PRION:CVE-2009-0799	
PRION:CVE-2009-0166	4.3	https://vulners.com/prion/PRION:CVE-2009-0166	
PRION:CVE-2009-0147	4.3	https://vulners.com/prion/PRION:CVE-2009-0147	
PRION:CVE-2009-0146	4.3	https://vulners.com/prion/PRION:CVE-2009-0146	
PRION:CVE-2008-5183	4.3	https://vulners.com/prion/PRION:CVE-2008-5183	
CVE-2014-2856	4.3	https://vulners.com/cve/CVE-2014-2856	
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	

## Просканируем через openvas

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

## Видим критическую уязвимость ssh

Deprecated SSH-1 Protocol Detection 7.5 (High)

### Summary

The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptographic flaws.

### Detection Result

The service is providing / accepting the following deprecated versions of the SSH protocol which have known cryptographic flaws:

1.33  
1.5

### Detection Method

Details: [Deprecated SSH-1 Protocol Detection OID: 1.3.6.1.4.1.25623.1.0.801993](#)  
Version used: 2023-03-24T10:19:42Z

### Affected Software/OS

Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

### Impact

Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

### Solution

**Solution Type:** Vendorfix  
Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

### References

CVE [CVE-2001-0361](#)  
[CVE-2001-0572](#)  
[CVE-2001-1473](#)  
CERT [DFN-CERT-2015-1619](#)  
[CB-K15/1534](#)  
Other <http://www.kb.cert.org/vuls/id/684820>  
<http://www.securityfocus.com/bid/2344>  
<http://xforce.iss.net/xforce/xfdb/6603>

Weak Host Key Algorithm(s) (SSH) 9.3 (Medium)

Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) 9.3 (Medium)

## Запустим Metasploit

```
(kali㉿kali)-[~]
└─$ sudo msfdb init && msfconsole
[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
Metasploit tip: Enable verbose logging with set VERBOSE true

IIIIII  dTb.dTb
 II     4'  v  'B
 II     6.    .P
 II     'T;. .;P'
 II     'T; ;P'
IIIIII 0000 'YvP'

I love shells --egypt

      =[ metasploit v6.3.51-dev ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 418 post ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

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

msf6 > 
```

Отообразим информацию по выбранной уязвимости и выполним настройку

```
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
wvu <wvu@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][ ... ]
RHOSTS           yes              yes        The target host(s), see https://docs.metasploit.com/docs/using-me
tasptloit/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 (timin
g 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
```

```

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-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 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file /usr/share/wordlists/metasploit/piata_ssh_userpass.t
xt
user_file => /usr/share/wordlists/metasploit/piata_ssh_userpass.txt

```

Результат выполнения эксплойта – список пользователей ssh dvl.

Рекомендация по исправлению – обновить OpenSSH до последней версии.

```

- SSH - Using malformed packet technique
- SSH - Checking for false positives
- SSH - Starting scan
- SSH - User 'root' found
- SSH - User 'mysql' found
- SSH - User 'ftp' found
- SSH - User 'nobody' found
- SSH - User 'news' found
- SSH - User 'games' found
- SSH - User 'mail' found
- SSH - User 'adm' found
- SSH - User 'operator' found
- SSH - User 'daemon' found
- SSH - User 'uucp' found

```

## Анализ полученных результатов

OpenVAS и Nmap - это инструменты для обнаружения уязвимостей в сети, но они имеют разные подходы и функциональность.

OpenVAS - это полноценная система управления уязвимостями, которая включает в себя OpenVAS-manager, OpenVAS-scanner и Greenbone-security-assistant. OpenVAS предлагает широкий спектр функций, таких как:

- Поиск уязвимостей на основе базы данных CVE
- Поиск уязвимостей с использованием скриптов NSE (Nmap Scripting Engine)
- Создание детальных отчетов о сети
- Поддержка различных политик сканирования

В то же время, OpenVAS является более сложным и глубоким инструментом, который может быть более уязвим к ошибкам и проблемам в сравнении с Nmap.

Nmap - это инструмент для обнаружения уязвимостей, который предоставляет более ограниченный набор функций, но может быть использоваться в сочетании с другими инструментами, такими как Vulners. Nmap может использоваться для обнаружения уязвимостей с помощью скриптов NSE, но его основная сила заключается в сканировании сети и обнаружении открытых портов и уязвимостей.

В нашем конкретном случае Nmap нашла значительно больше уязвимостей, однако основная причина в OpenvVAS включен скудный набор параметров сканирования по умолчанию.

Как OpenVAS, так и Nmap являются инструментами с открытым исходным кодом, что позволяет пользователям свободно использовать их для обнаружения уязвимостей.

В целом, OpenVAS предлагает более полную функциональность для управления уязвимостями, включая создание детальных отчетов и поддержку

различных политик сканирования. В то же время, Nmap может быть использоваться для обнаружения уязвимостей с помощью скриптов NSE, но его функциональность ограничена сканированием сети и обнаружением открытых портов. Также Nmap значительно более быстра, что дает ей преимущество при поиске уязвимостей в большой сети.

В итоге, оба инструмента лучше использовать вместе для более полного обнаружения уязвимостей. Например, результаты, полученные с помощью Nmap, могут быть использованы в OpenVAS для более глубокого анализа уязвимостей.

Metasploit — это мощный фреймворк для исследования уязвимостей в сетях и приложениях, который может быть использован как киберпреступниками, так и специалистами по информационной безопасности. Он предоставляет широкий спектр инструментов для сканирования, обнаружения уязвимостей, эксплуатации и управления безопасностью. Metasploit Framework является открытым исходным кодом и может быть легко настроен и использован на большинстве операционных систем. Он также предлагает готовые модули и возможность создания собственных надстроек. Metasploit широко используется специалистами по безопасности для проверки уровня защиты сетей и приложений.