

Технический аудит.

Лабораторная работа №1.

- 1. Подготовка тестовой среды, установка виртуальную машину с ОС Kali Linux и виртуальную машину с уязвимостями "metasploitable 2"**

Цель:

установить на локальную машину виртуальную машину с ОС Kali Linux и виртуальную машину с уязвимостями "metasploitable 2", работа с которыми будет проводиться в последующих работах.

По окончании работы студент должен:

1. Знать: как работать с виртуальными машинами
2. Уметь: устанавливать виртуальные машины.

Задание:

1. установить программу виртуализации Virtual Box
2. установить виртуальной машины Kali Linux
3. Установить виртуальную машину Metasploitable 2

Технические инструменты для выполнения работы

1. Программа виртуализации Virtual Box
2. Виртуальная машина Kali Linux
3. Виртуальная машина Metasploitable 2

Ссылки:

<https://www.virtualbox.org/wiki/Downloads>

<https://www.kali.org/get-kali/#kali-virtual-machines>

<https://sourceforge.net/projects/metasploitable/files/latest/download>

Порядок выполнения работ

Для создания тестовой среды рекомендуется использовать компьютер со следующими характеристиками:

1. Компьютер с современным 4 (или более) ядерным процессором Intel или AMD;
2. Оперативная память – 8 ГБ и более;
3. Дисковое пространство от 256 ГБ.

(Возможно использование компьютеров с менее мощными характеристиками).

1.1. Установка программы виртуализации **Virtual Box**

Для установки программы виртуализации Virtual Box, для операционных систем Windows, необходимо выполнить следующие действия:

Скачать программу виртуализации Virtual Box по ссылке:

<https://www.virtualbox.org/wiki/Downloads>



Рис. 1.1 Страница загрузки программы виртуализации Virtual Box.

Установите программу виртуализации Virtual Box, запустив скачанный файл VirtualBox-7.1.6-167084-Win.exe.

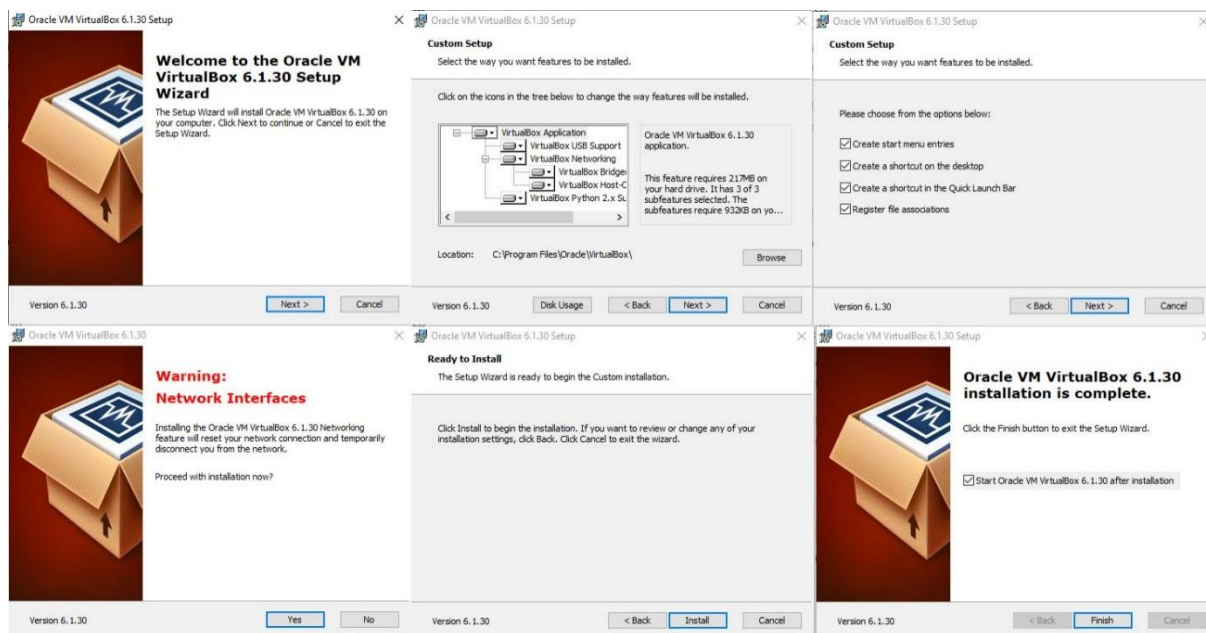


Рис. 1.2 Установка программы виртуализации Virtual Box.

После установки VirtualBox вы можете столкнуться с проблемой невозможности выбрать профиль для установки 64-битных опций для операционных систем, когда в выпадающем меню выбора версии ОС будут доступны только 32-битные опции.

Причина исчезновения 64-битных вариантов операционных систем в VirtualBox чаще всего связана с отключенной функцией аппаратной виртуализации центрального процессора компьютера. Стоит отметить, что данная опция включена не в операционной системе, а исключительно в опциях BIOS компьютера.

Необходимо зайти в BIOS вашего компьютера, найти там опцию под названием Intel Virtual Technology (для процессоров Intel), SVM Mode (для процессоров AMD) или что-то подобное (в зависимости от типа BIOS и производителя процессора) и переключить ее в состояние Enabled.

1. Установка виртуальной машины Kali Linux

По ссылке <https://www.kali.org/get-kali/#kali-virtual-machines> скачать архив kali-linux-2024.4-virtualbox-amd64.7z с образом виртуальной машины kali-linux.

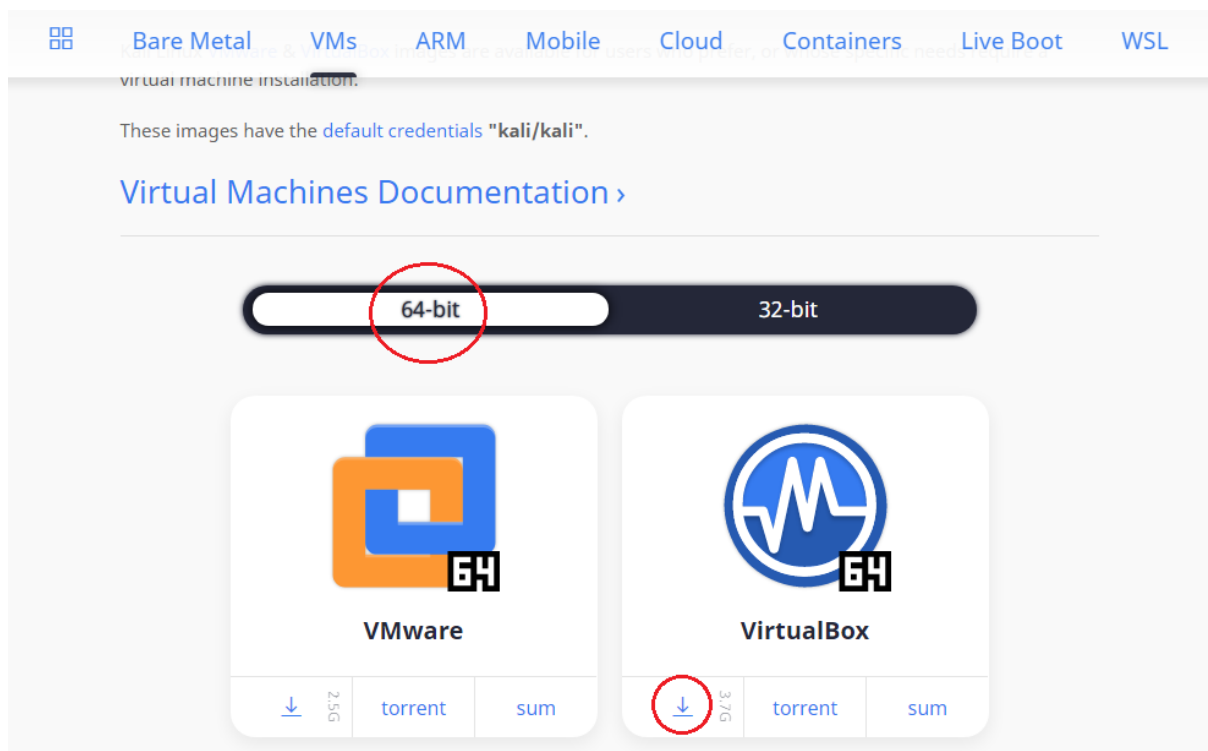


Рис. 1.2 Страница загрузки образа виртуальной машины Kali Linux.

Распаковать архив kali-linux-2024.4-virtualbox-amd64.7z.

Чтобы установить образ виртуальной машины Kali Linux, выполните следующие действия:

1. В программе виртуализации Virtual Box выберите в меню «Файл», «Импорт конфигураций».
2. Выберите распакованный образ виртуальной машины Kali Linux.
3. Импортируйте образ виртуальной машины Kali Linux.

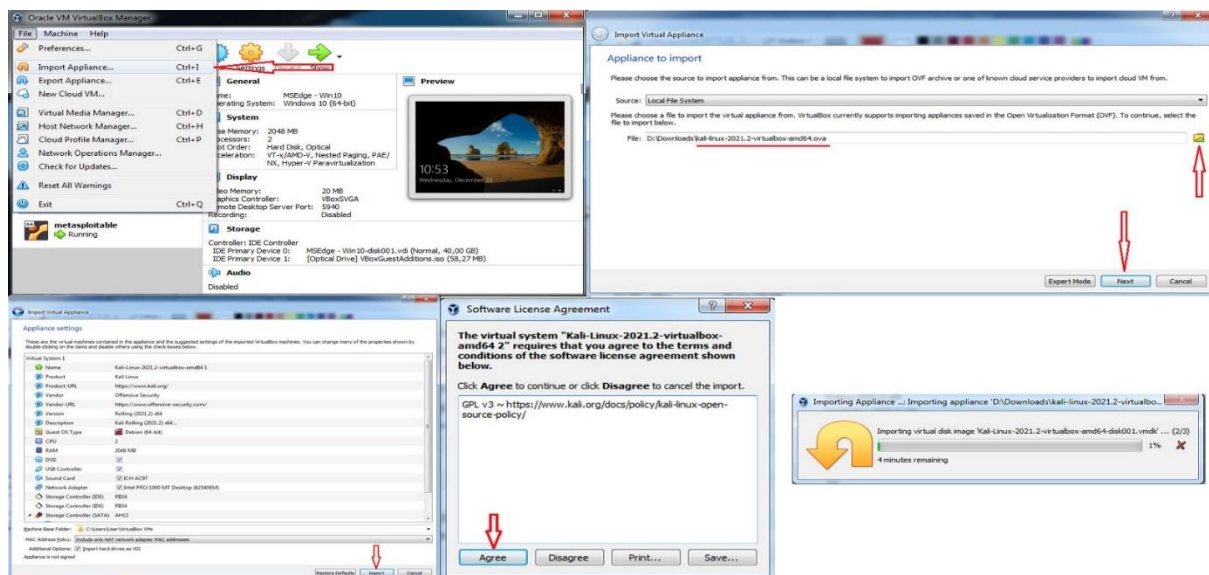


Рис. 1.2 Импорт образа виртуальной машины в Virtual Box.

В настройках созданной виртуальной машины выберите пункт «Сеть», а в параметре «Подключено к» выберите «Bridged Adapter», а в параметре «Name» выберите имя вашего сетевого адаптера, через который осуществляется подключение к интернету.

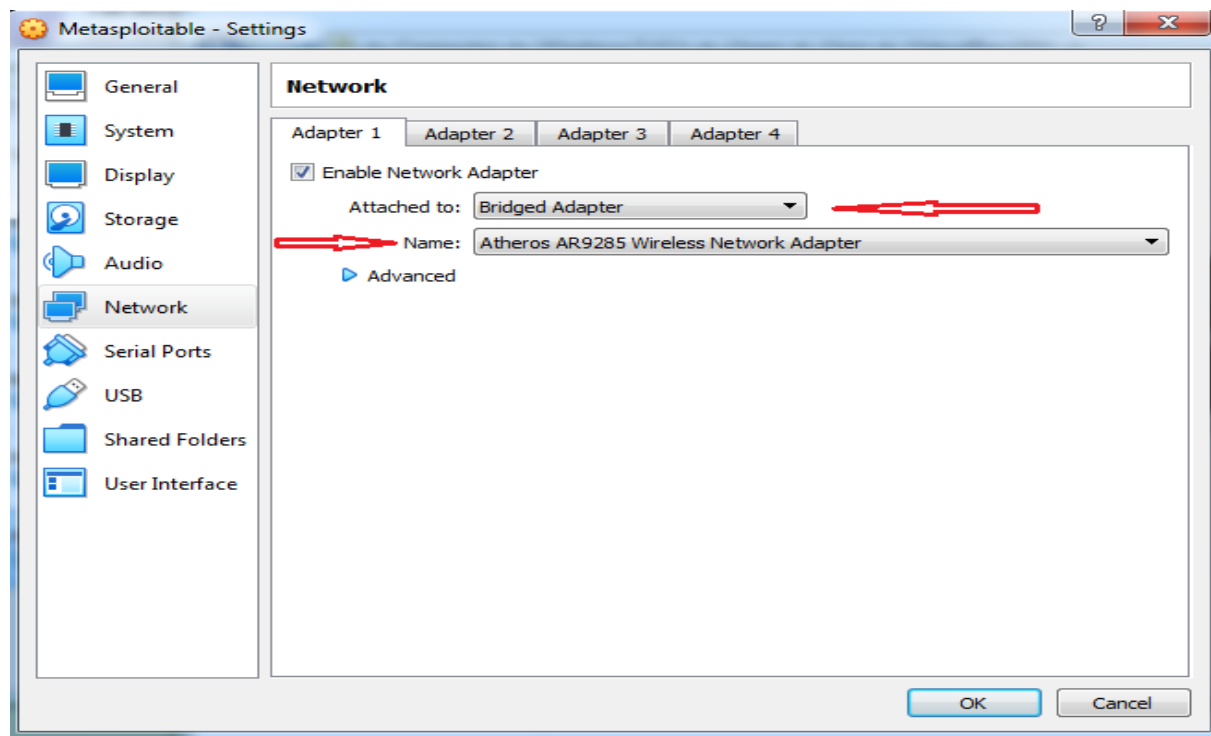


Рис. 1.3 Настройка сетевого адаптера виртуальной машины Kali linux.

Чтобы запустить виртуальную машину Kali linux, нажмите кнопку «Запустить».

Чтобы войти в виртуальную машину Kali linux, введите логин kali и пароль kali.

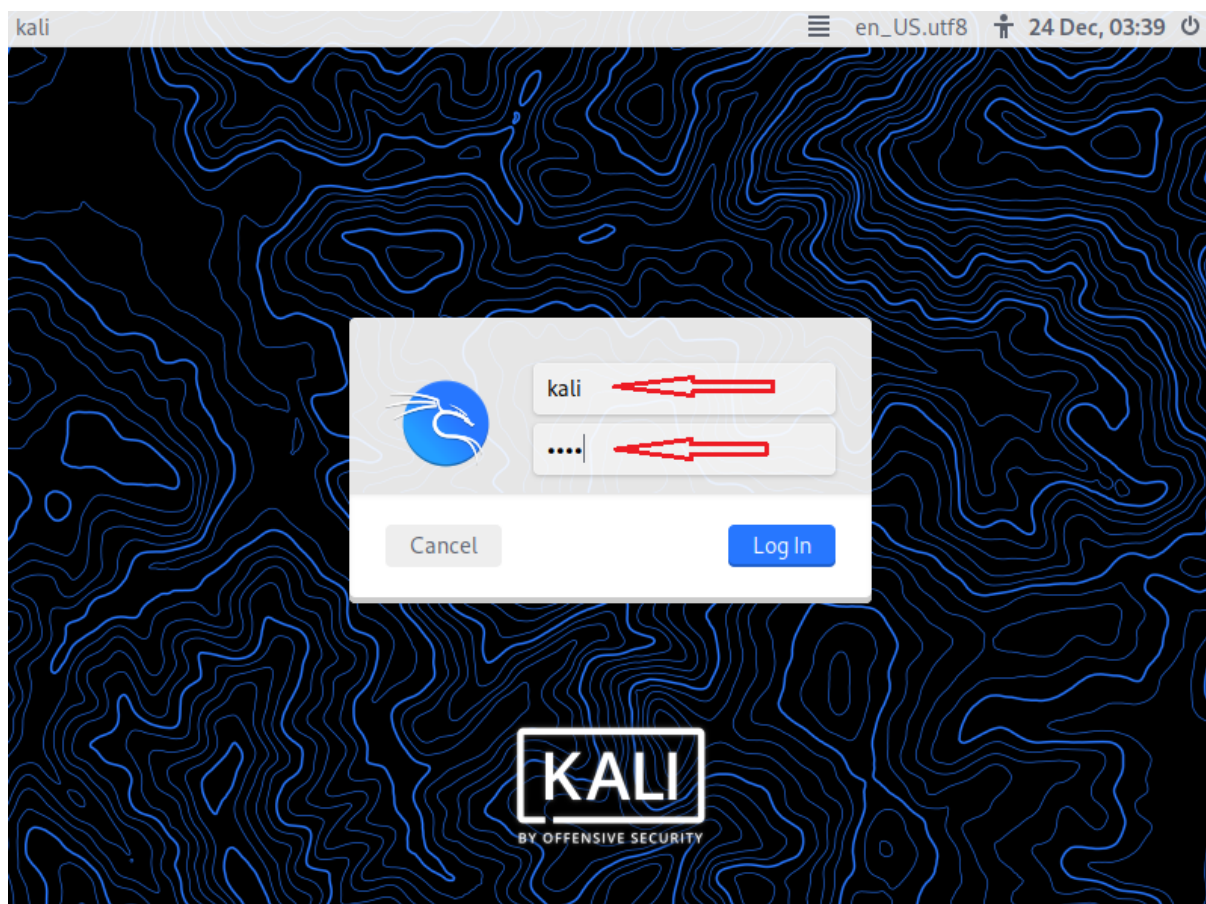
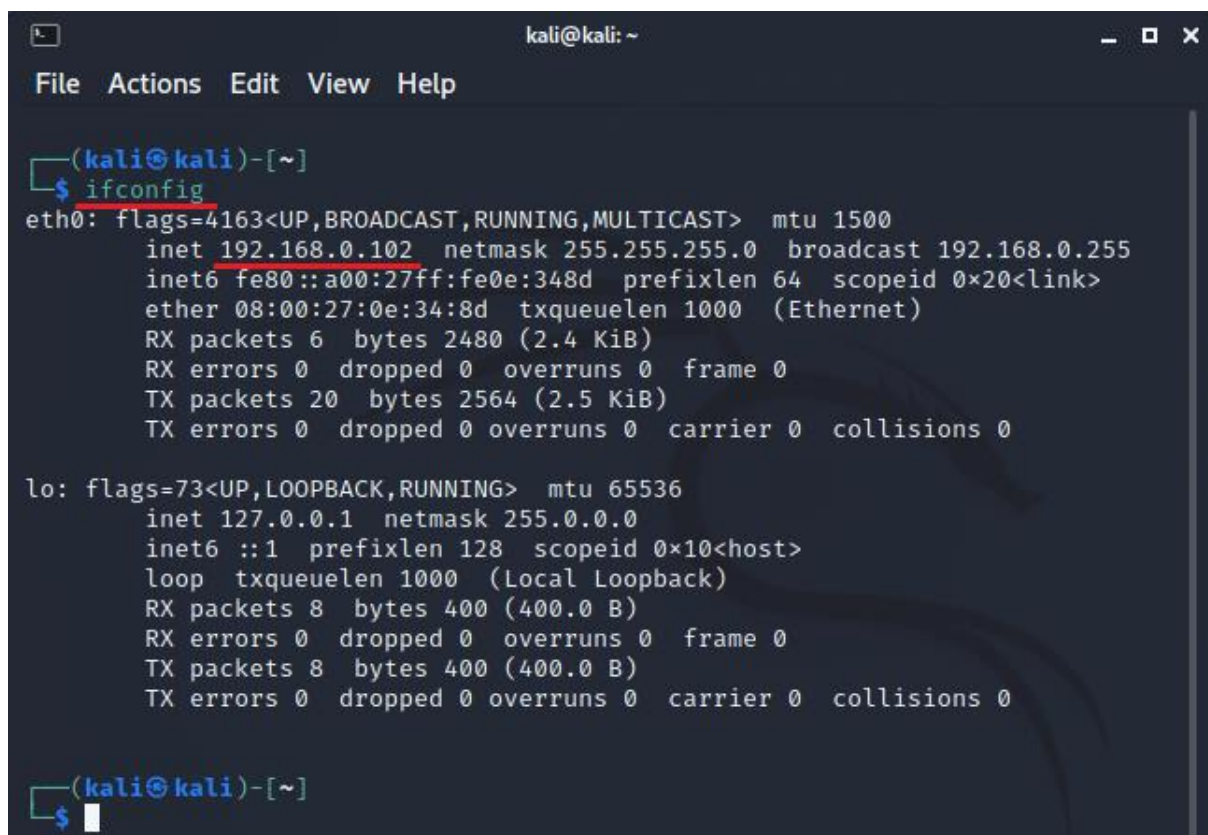


Рис. 1.4 Консоль входа в виртуальную машину Kali linux.

Чтобы определить IP-адрес, полученный виртуальной машиной Kali linux, введите команду `ifconfig`.



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

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.102 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe0e:348d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0e:34:8d txqueuelen 1000 (Ethernet)
    RX packets 6 bytes 2480 (2.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 2564 (2.5 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 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

Рис. 1.5 Определение IP-адреса виртуальной машины Kali linux.

Для корректной работы вашей операционной системы на Kali linux, необходимо выполнить обновление, для этого в терминале выполните следующие команды:

```
sudo apt update
```

```
sudo apt upgrade -y
```

1.2. Установка виртуальной машины metasploitable 2

По ссылке <https://sourceforge.net/projects/metasploitable/files/latest/download> скачать архив metasploitable-linux-2.0.0.zip с образом виртуальной машины metasploitable 2.

Разархивировать архив metasploitable-linux-2.0.0.zip.

Запустить программу Oracle VM VirtualBox.

- Выберите в меню пункт NEW.
- Введите имя виртуальной машины (имя может быть любым), например “metasploitable”.

1. Выбрать тип виртуальной машины - Linux

- Выбрать версию Linux – Ubuntu(64-bit)
- Выбрать размер оперативной памяти, рекомендуется 1024Mb.
- Выбрать виртуальный диск, для этого:
 - Выберите пункт “Use an existing virtual hard disk file” и щелкните значок желтой папки.
 - В следующем окне выбрать пункт “Add” и выбрать файл Metasploitable.vmdk в папке, в которой разархивирован архив с виртуальной машиной metasploitable 2.
 - В открывшемся окне выбрать Metasploitable.vmdk и нажать кнопку “Choose”.
 - В следующем окне нажать кнопку “Create”.

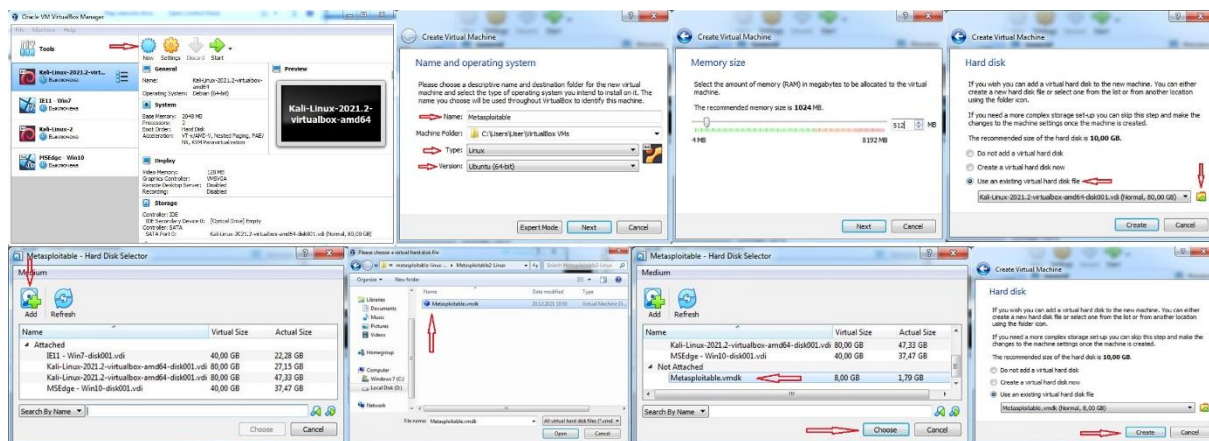


Рис. 1.3 Установка виртуальной машины metasploitable 2.

В настройках созданной виртуальной машины выберите пункт “Network”, и в “Attached to” выбрать “Bridged Adapter”, а в “Name” выбрать название своего сетевого адаптера, через который происходит соединение с интернетом.

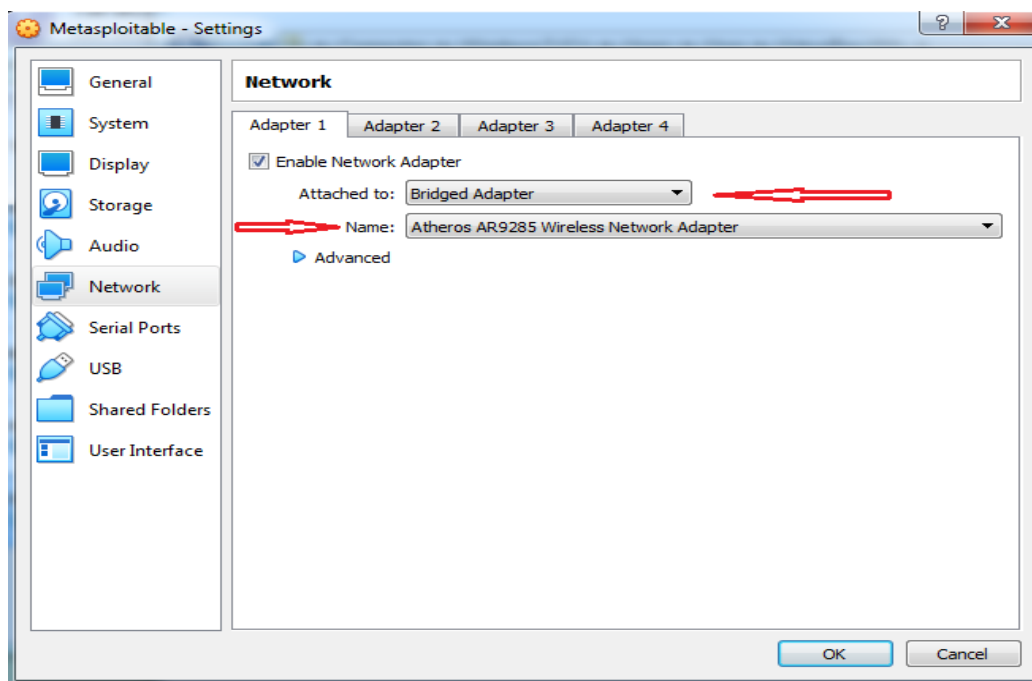


Рис. 1.3 Настройка сетевого адаптера виртуальной машины metasploitable 2.

Для запуска виртуальной машины metasploitable 2 нажмите кнопку “Start”.

Для входа в виртуальную машину metasploitable 2 введите логин **msfadmin** и пароль **msfadmin**.

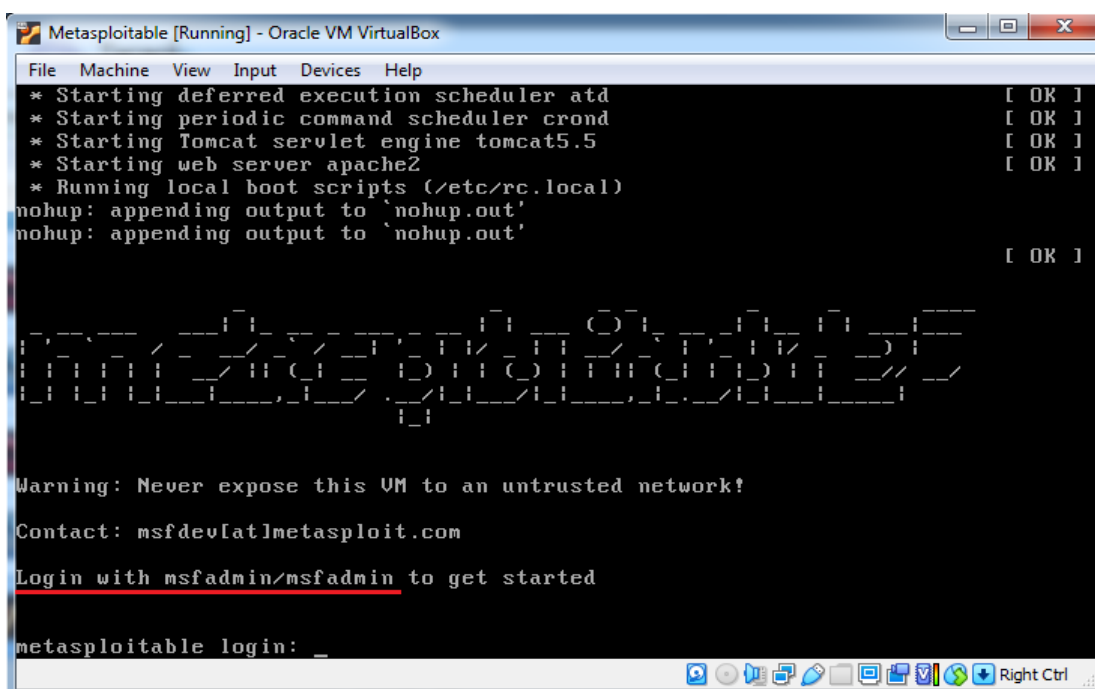


Рис. 1.4 Консоль входа в виртуальную машину metasploitable 2.

Для определения IP адреса, получившего виртуальную машину metasploitable 2, введите команду `ifconfig`.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:81:0b:67
          inet addr:192.168.0.103  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe81:b67/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4130 (4.0 KB)  TX bytes:6210 (6.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$ _
```

Рис. 1.5 Определение IP-адреса виртуальной машины metasploitable 2.

Для правильной работы веб-сервиса “mutillidae” на виртуальной машине metasploitable 2 необходимо проверить, правильно ли указано название базы данных в конфигурационном файле `config.inc`, находящемся в папке `/var/www/mutillidae`, для этого введем следующую команду:

```
sudo nano /var/www/mutillidae/config.inc
```

Если в строке `$dbname = 'owasp10'`, вместо 'owasp10' указано другое название, замените его на 'owasp10' и сохраните файл.

После этого необходимо перезагрузить веб-сервер Apache, для этого введите команду:

```
sudo /etc/init.d/apache2 restart
```