

Lab 1.1 Kali Linux installation into the VirtualBox

Type of the lab: local

Prerequisites:

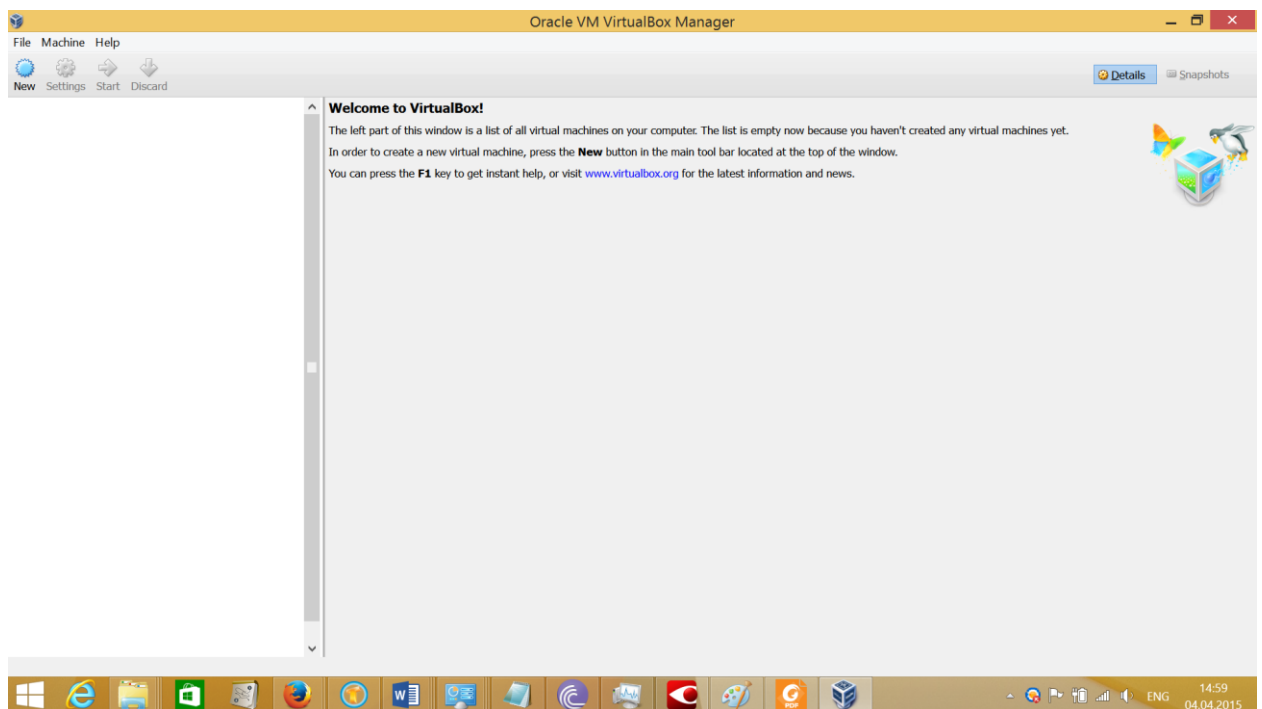
- 1) Kali Linux ISO-image
- 2) VirtualBox Software installed

Task:

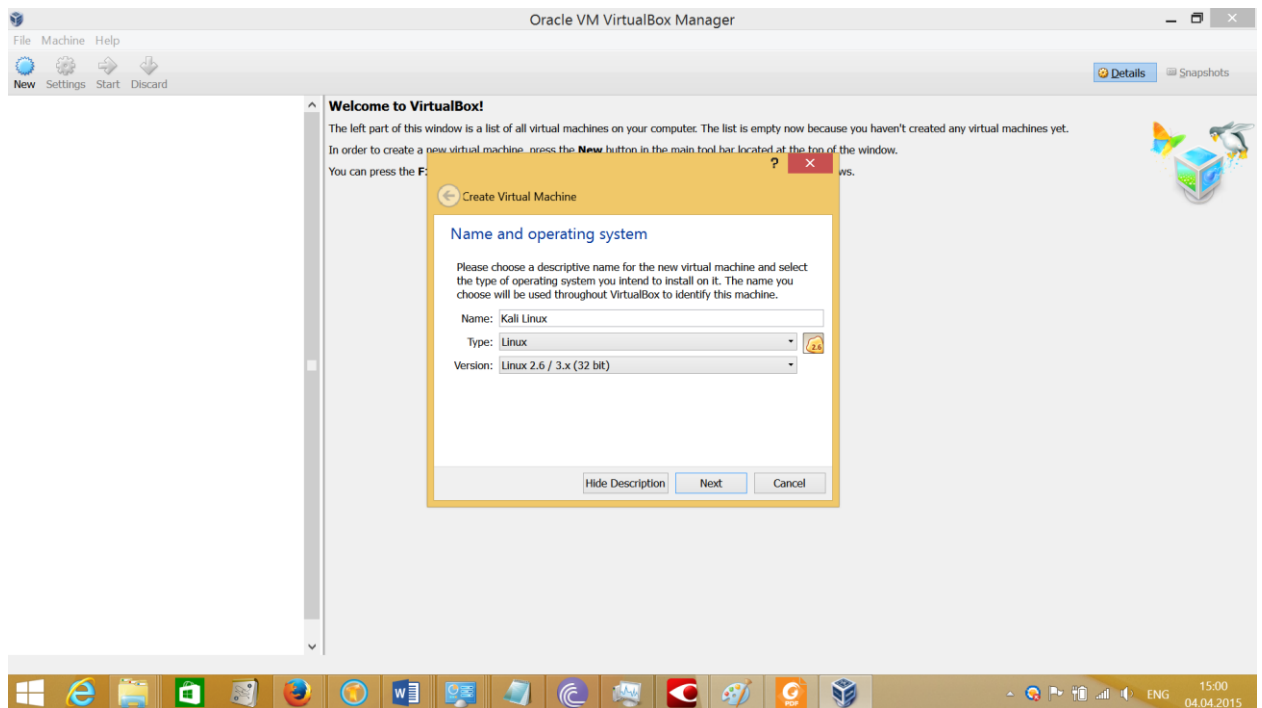
- 1) Create Kali Linux virtual machine
- 2) Install VirtualBox add-ons
- 3) Update the system

Solution

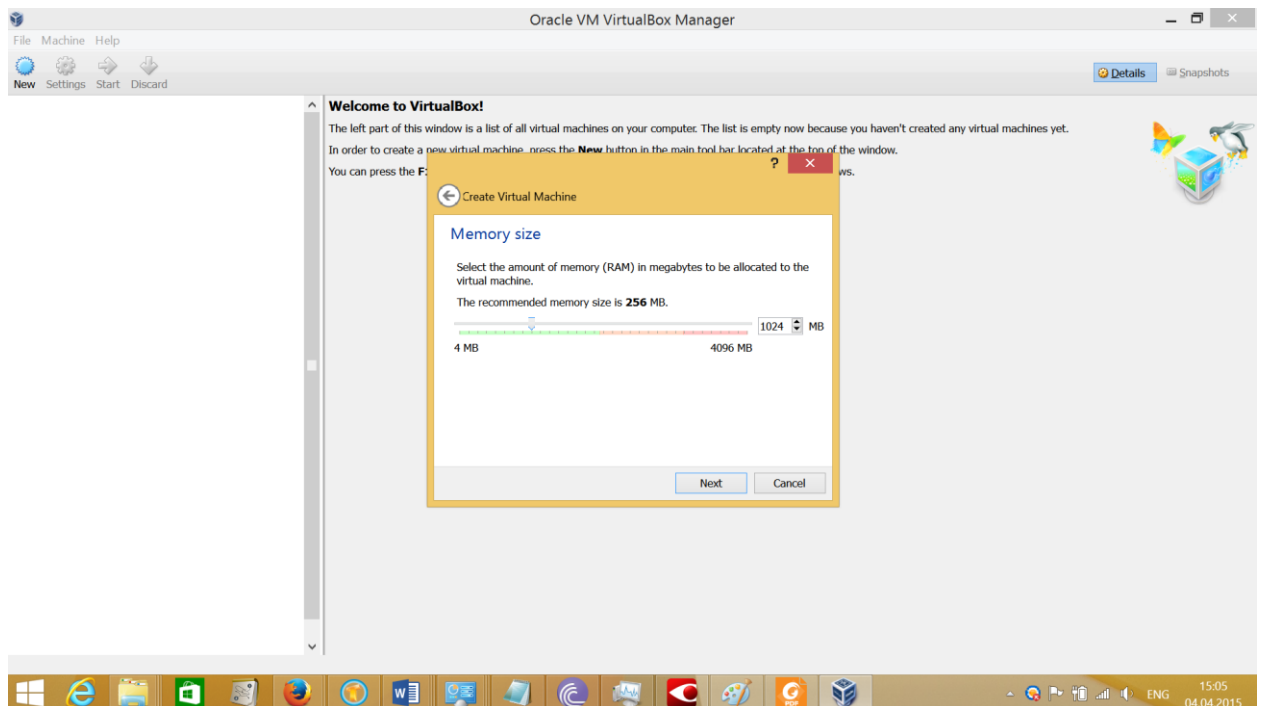
- 1) Run Virtual Box



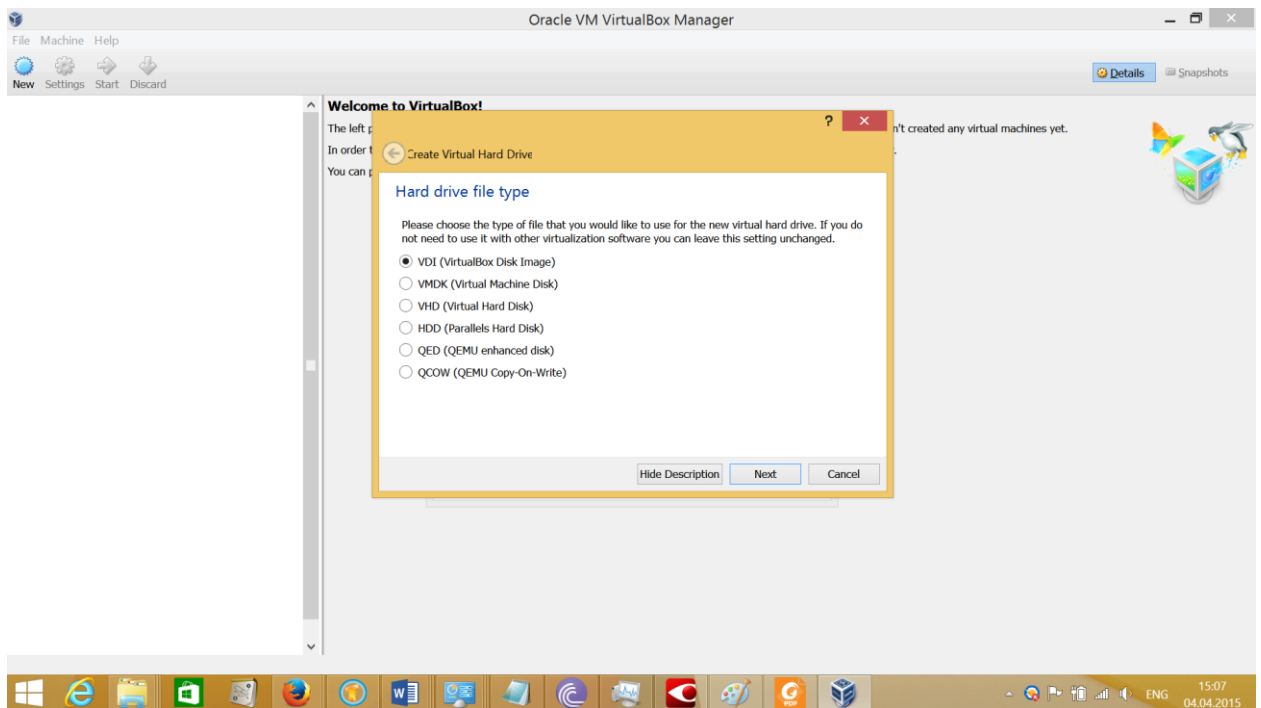
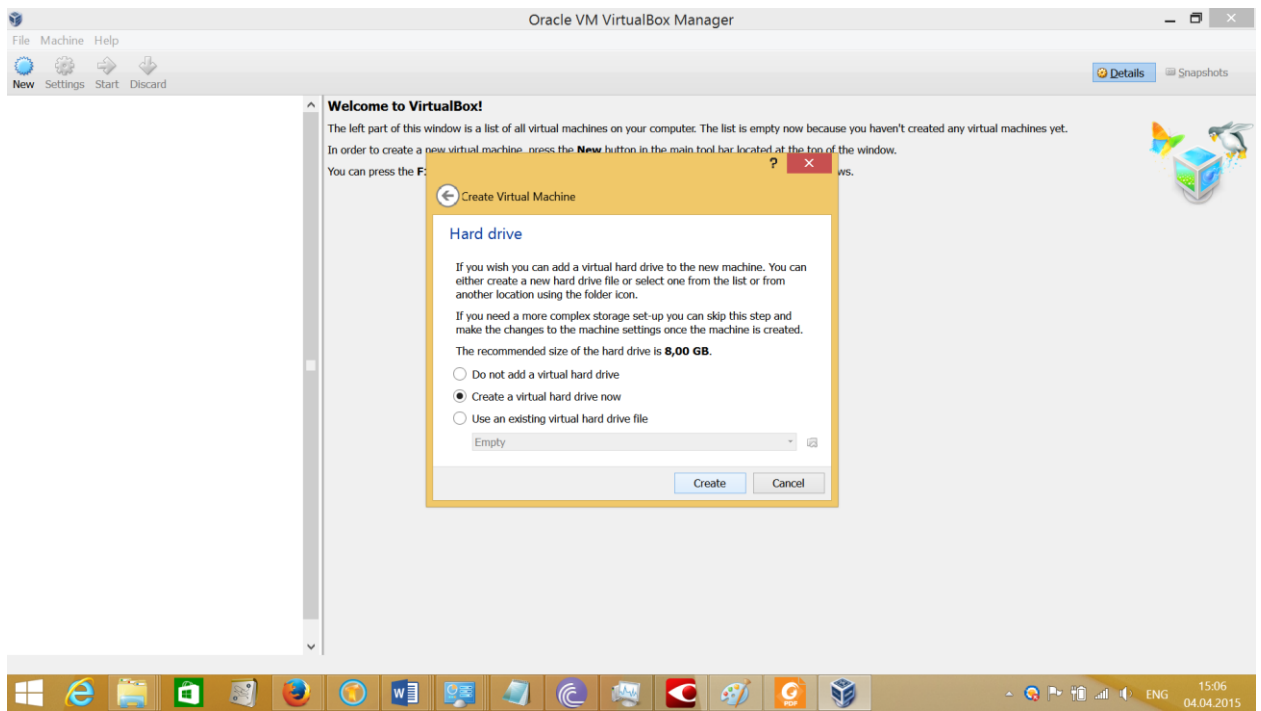
- 2) Machine->New
- 3) Set name of the machine and corresponding parameters depending on the type of ISO image of Kali Linux you have

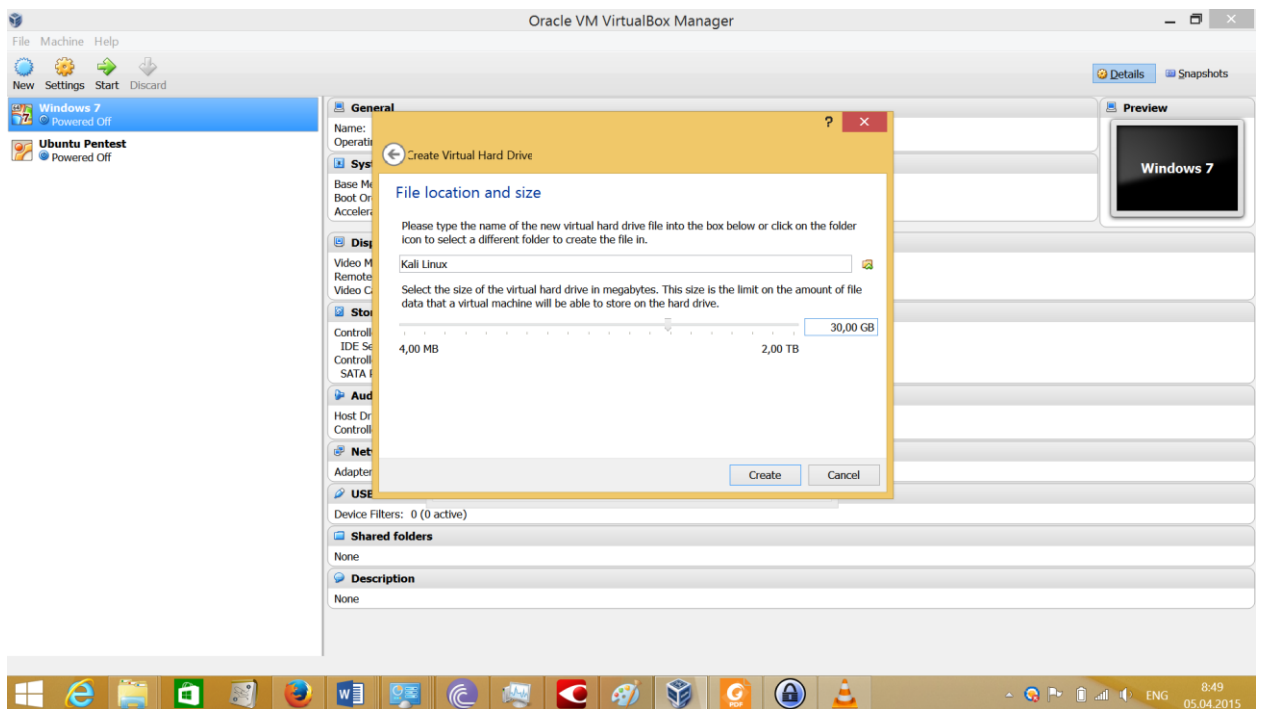
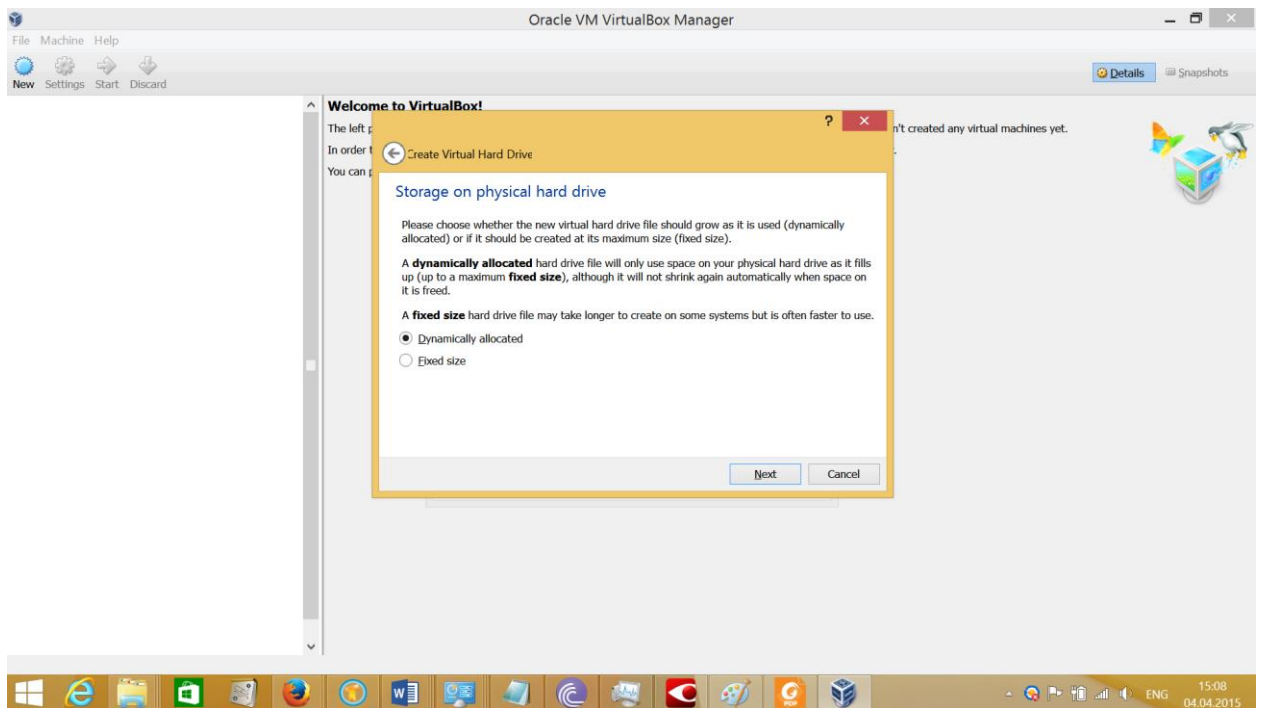


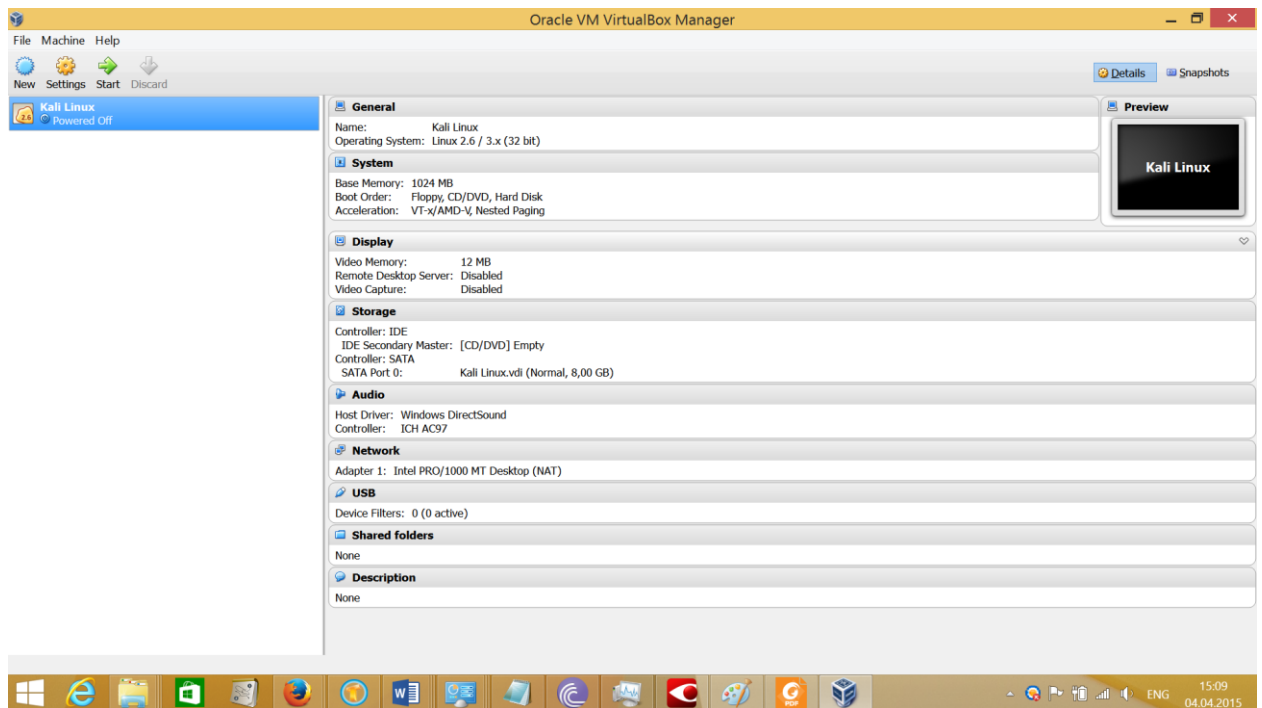
4) Set memory size **1GB**



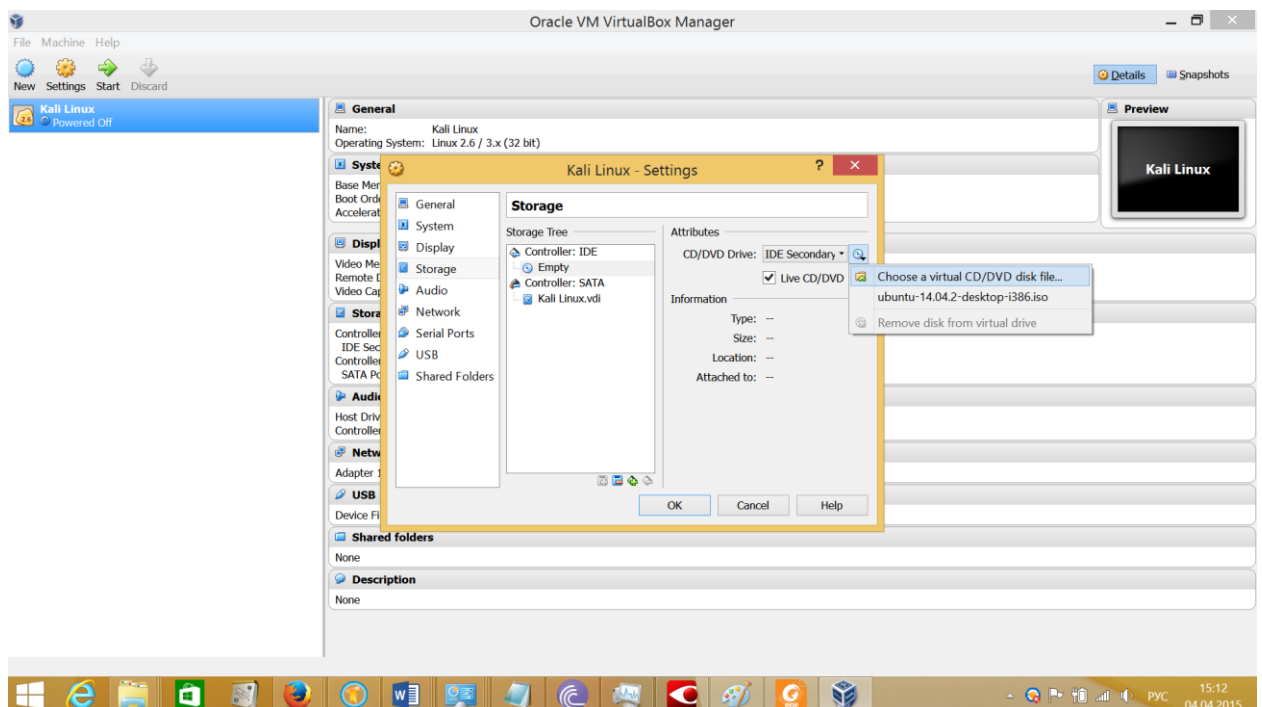
1) Create virtual hard drive. **Set size 30 GB.**



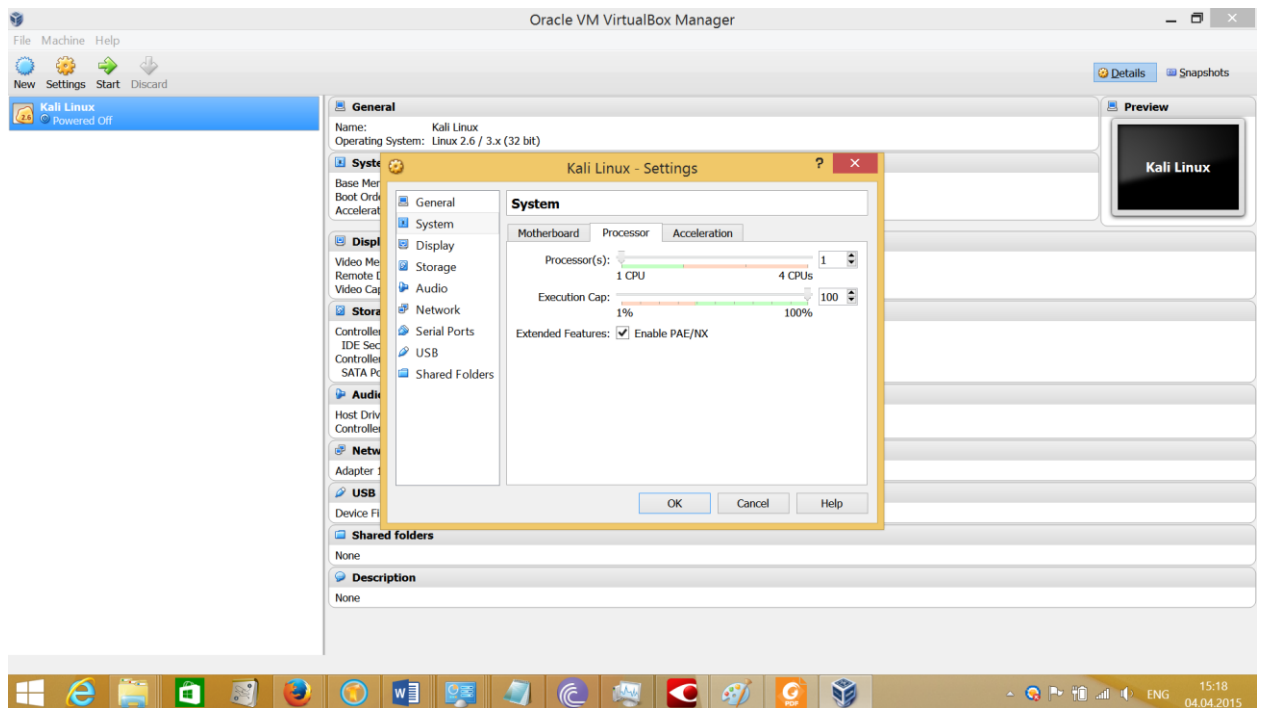




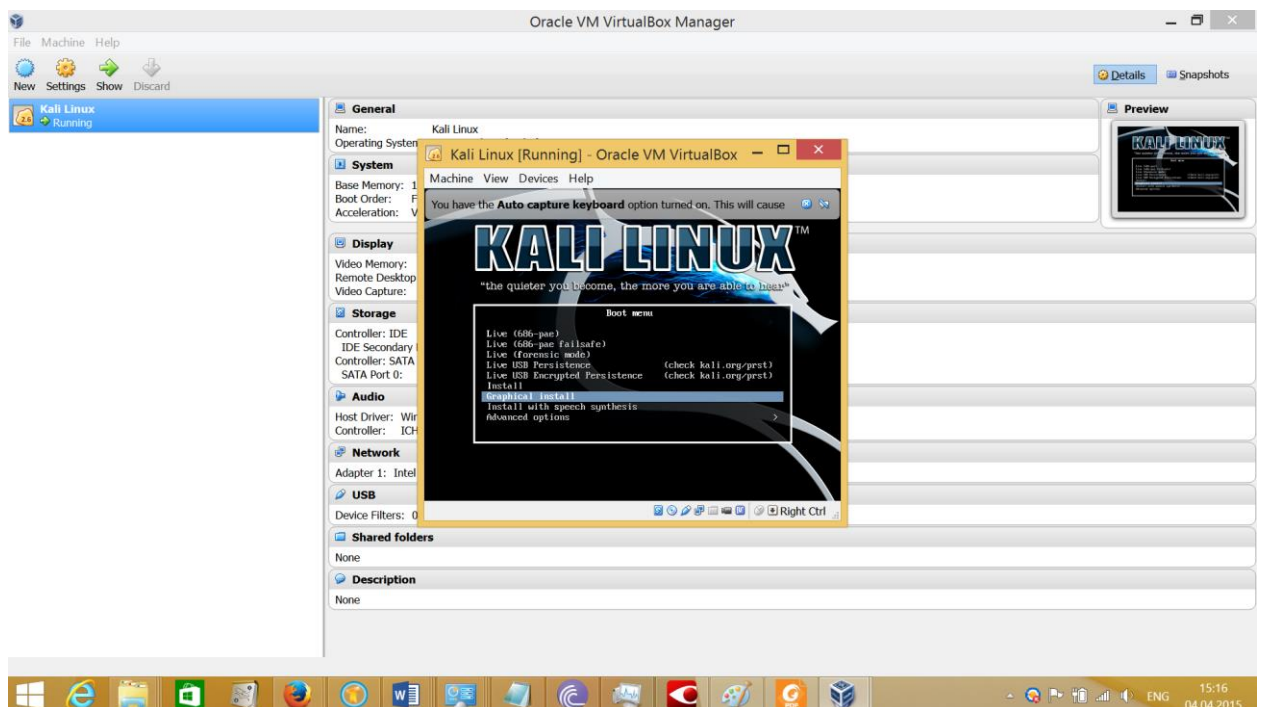
- 1) Run the system from the live CD (Kali Linux image): click settings of the machine, set Live CD/DVD option and choose Kali Linux ISO image.



- 2) Enable PAE: System->Processor



- 3) Start the Virtual Machine
- 4) Choose Graphical Install

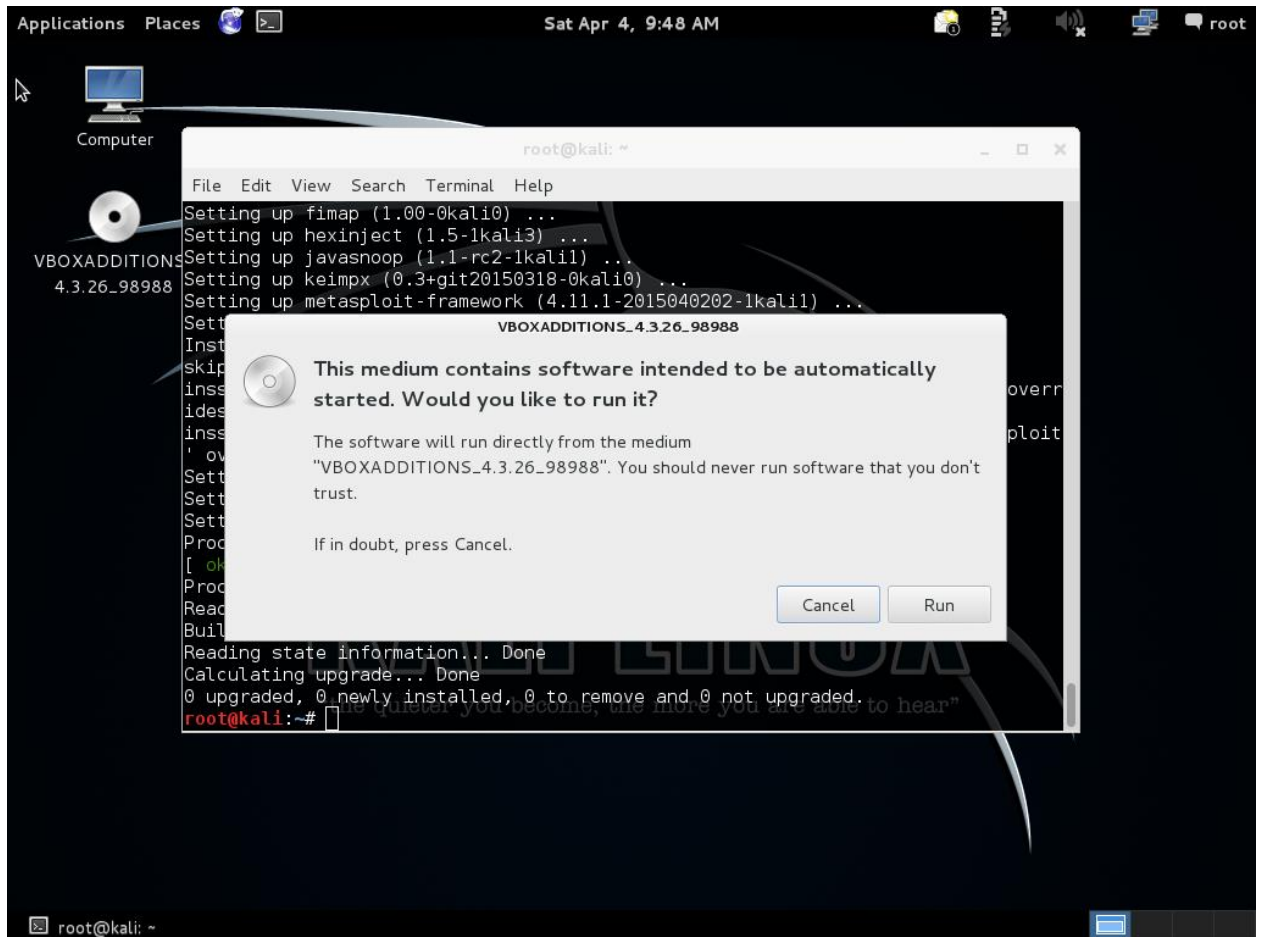


VirtualBox addons installation

- 1) Start up your Kali Linux virtual machine, open a terminal window and issue the following command to install the Linux kernel headers.

`apt-get update && apt-get install -y linux-headers-$(uname -r)`

Once this is complete you can now attach the “Guest Additions” CD-ROM image. Select “Devices” from the VirtualBox menu and then select “Install Guest Additions”. This will mount the Guest Additions ISO in the virtual CD drive in your Kali Linux virtual machine. When prompted to autorun the CD, click the Cancel button.



From a terminal window, copy the VBoxLinuxAdditions.run file from the Guest Additions CD-ROM to a path on your local system. Ensure it is executable and run the file to begin the installation.

```
cp /media/cdrom/VBoxLinuxAdditions.run /root/
```

```
chmod 755 /root/VBoxLinuxAdditions.run
```

```
cd /root
```

```
./VBoxLinuxAdditions.run
```

Lab 1.2 Kali Linux exploration

Task:

- 1) Determine the location of the file nmap in Kali
- 2) Find and read the documentation for the nmap tool

Solution


```
root@kali:~# updatedb
root@kali:~# locate nmap
```



The image shows a Kali Linux desktop environment. A terminal window is open, displaying the output of the 'locate nmap' command. The output lists various files and directories associated with Nmap, including paths like /opt/metasploit/apps/pro/vendor/bundle/ruby/2.1.0/gems/metasploit_data_models-0.23.2/app/models/metasploit_data_models/ip_address/v4/segment/nmap/list.rb, /usr/bin/nmap, and /usr/bin/nmap_client. The desktop background features the Kali Linux logo and the text 'KALI LINUX™' and '“the quieter you become, the more you are able to hear”'. The system clock in the top right corner shows 'Sat Apr 4, 10:21 AM'.

```
root@kali:~# locate nmap
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.1.0/gems/metasploit_data_models-0.23.2/app/models/metasploit_data_models/ip_address/v4/segment/nmap/list.rb
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.1.0/gems/metasploit_data_models-0.23.2/app/models/metasploit_data_models/ip_address/v4/segment/nmap/range.rb
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.1.0/gems/metasploit_data_models-0.23.2/spec/app/models/metasploit_data_models/ip_address/v4/nmap_spec.rb
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.1.0/gems/metasploit_data_models-0.23.2/spec/app/models/metasploit_data_models/ip_address/v4/segment/nmap
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.1.0/gems/metasploit_data_models-0.23.2/spec/app/models/metasploit_data_models/ip_address/v4/segment/nmap/list_spec.rb
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.1.0/gems/metasploit_data_models-0.23.2/spec/app/models/metasploit_data_models/ip_address/v4/segment/nmap/range_spec.rb
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.1.0/gems/metasploit_data_models-0.23.2/spec/factories/edm/fingerprints/nmap_fingerprints.rb
/usr/bin/dnmap_server
/usr/bin/dnmap_client
/usr/bin/nmap
/usr/bin/nmapfe
/usr/bin/xnmap
/usr/bin/zenmap
/usr/include/glib-2.0/gio/gactionmap.h
/usr/lib/nmap
```

```
root@kali:~# man nmap
```



The image shows a Kali Linux desktop environment. A terminal window is open, displaying the man page for 'nmap'. The man page includes sections for NAME, SYNOPSIS, and DESCRIPTION. The NAME section states 'nmap - Network exploration tool and security / port scanner'. The SYNOPSIS section shows 'nmap [Scan Type...] [Options] (target specification)'. The DESCRIPTION section provides a detailed overview of Nmap, stating it is an open source tool for network exploration and security auditing. The desktop background features the Kali Linux logo and the text 'KALI LINUX™' and '“the quieter you become, the more you are able to hear”'. The system clock in the top right corner shows 'Sat Apr 4, 10:23 AM'.

```
root@kali:~# man nmap
NAME
nmap - Network exploration tool and security / port scanner

SYNOPSIS
nmap [Scan Type...] [Options] (target specification)

DESCRIPTION
Nmap ("Network Mapper") is an open source tool for network exploration
and security auditing. It was designed to rapidly scan large networks,
although it works fine against single hosts. Nmap uses raw IP packets
in novel ways to determine what hosts are available on the network,
what services (application name and version) those hosts are offering,
what operating systems (and OS versions) they are running, what type of
packet filters/firewalls are in use, and dozens of other
characteristics. While Nmap is commonly used for security audits, many
systems and network administrators find it useful for routine tasks
such as network inventory, managing service upgrade schedules, and
monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental
information on each depending on the options used. Key among that
Manual page nmap(1) line 1 (press h for help or q to quit)
```