

GL<>Wipro CRS NGA - SIA C2 - Graded Project 2

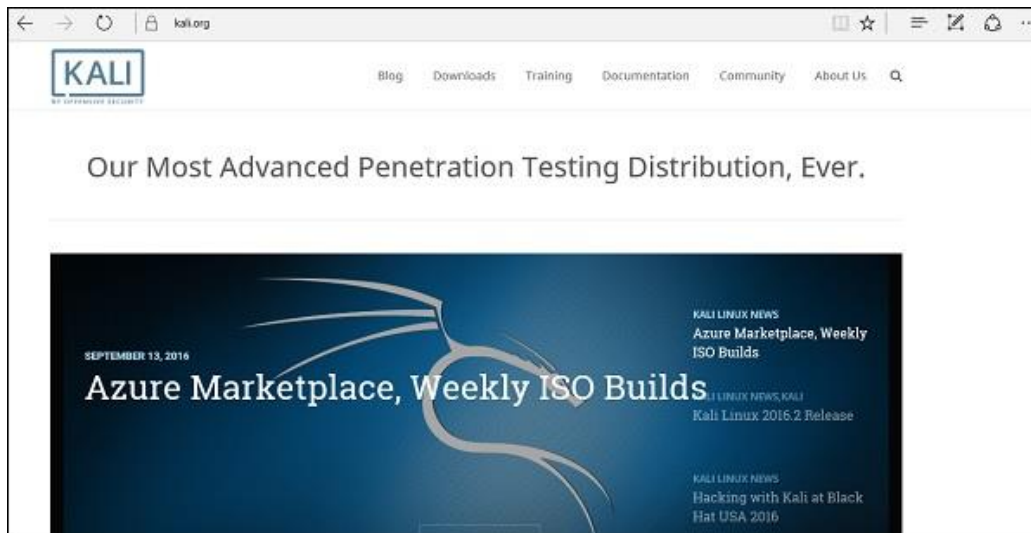
Kali Linux Tools - Project Brief

What is Kali Linux?

Kali Linux is one of the best open-source security packages of an ethical hacker, containing a set of tools divided by categories. Kali Linux can be installed in a machine as an Operating System, which is discussed in this tutorial. Installing Kali Linux is a practical option as it provides more options to work and combine the tools.

Kali Linux is one of the best security packages of an ethical hacker, containing a set of tools divided by the categories. It is an open source and its official webpage is <https://www.kali.org>.

Generally, Kali Linux can be installed in a machine as an Operating System, as a virtual machine which we will discuss in the following section. Installing Kali Linux is a practical option as it provides more options to work and combine the tools. You can also create a live boot CD or USB. All this can be found in the following link: <https://www.kali.org/downloads/>



To install Kali Linux –

- First, we will download the Virtual box and install it.
- Later, we will download and install Kali Linux distribution.

Download and Install the Virtual Box

A Virtual Box is particularly useful when you want to test something on Kali Linux that you are unsure of. Running Kali Linux on a Virtual Box is safe when you want to experiment with unknown packages or when you want to test a code.

With the help of a Virtual Box, you can install Kali Linux on your system (not directly in your hard disk) alongside your primary OS which can MAC or Windows or another flavor of Linux.

Let's understand how you can download and install the Virtual Box on your system.

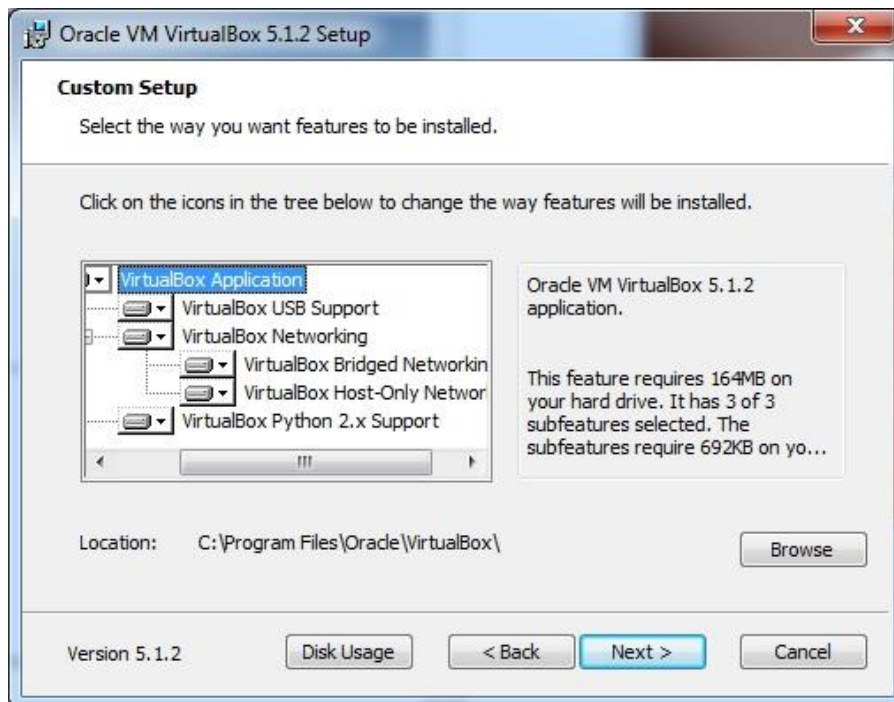
Step 1 – To download, go to <https://www.virtualbox.org/wiki/Downloads>. Depending on your operating system, select the right package. In this case, it will be the first one for Windows as shown in the following screenshot.



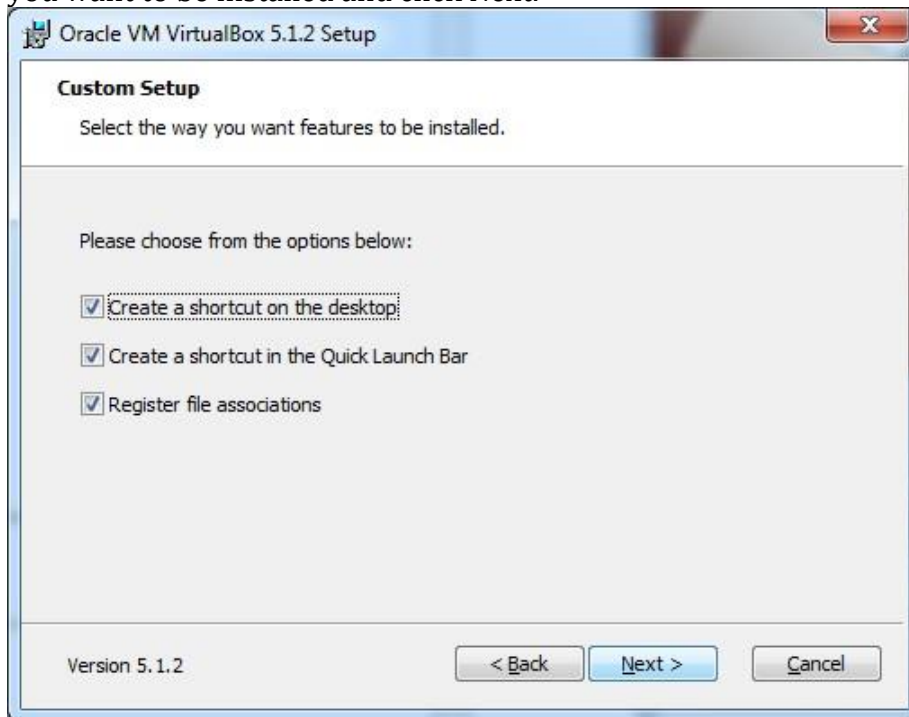
Step 2 – Click Next.



Step 3 – The next page will give you options to choose the location where you want to install the application. In this case, let us leave it as default and click **Next**.



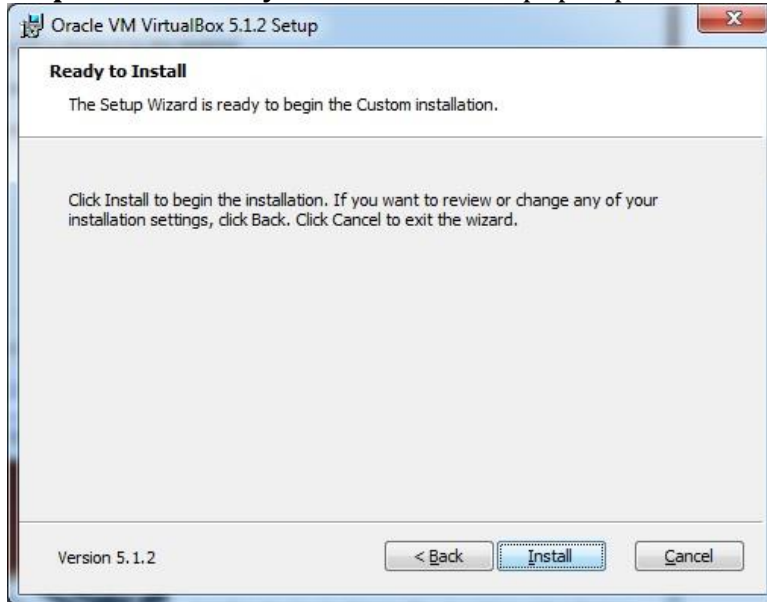
Step 4 – Click **Next** and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click Next.



Step 5 – Click **Yes** to proceed with the installation.



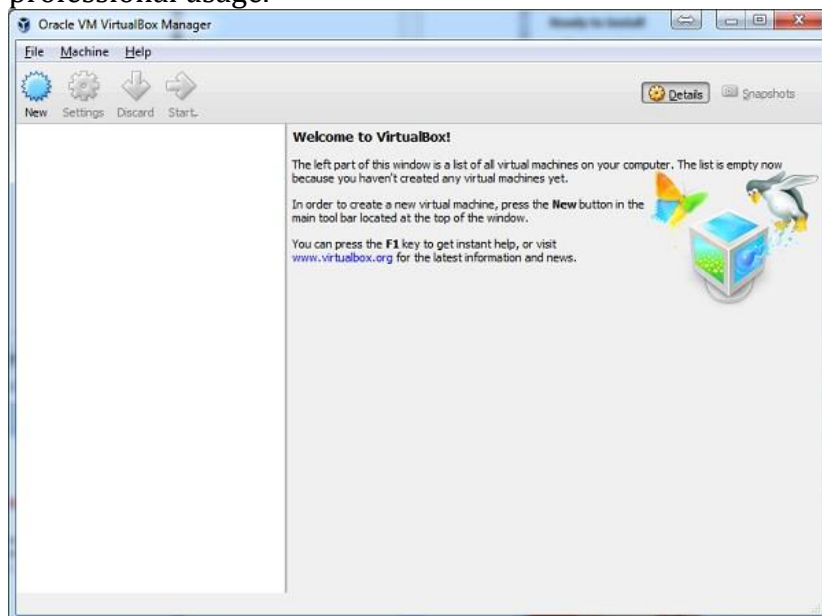
Step 6 – The Ready to Install screen pops up. Click Install.



Step 7 – Click the Finish button.



The Virtual Box application will now open as shown in the following screenshot. Now we are ready to install the rest of the hosts for this manual and this is also recommended for professional usage.



Install Kali Linux

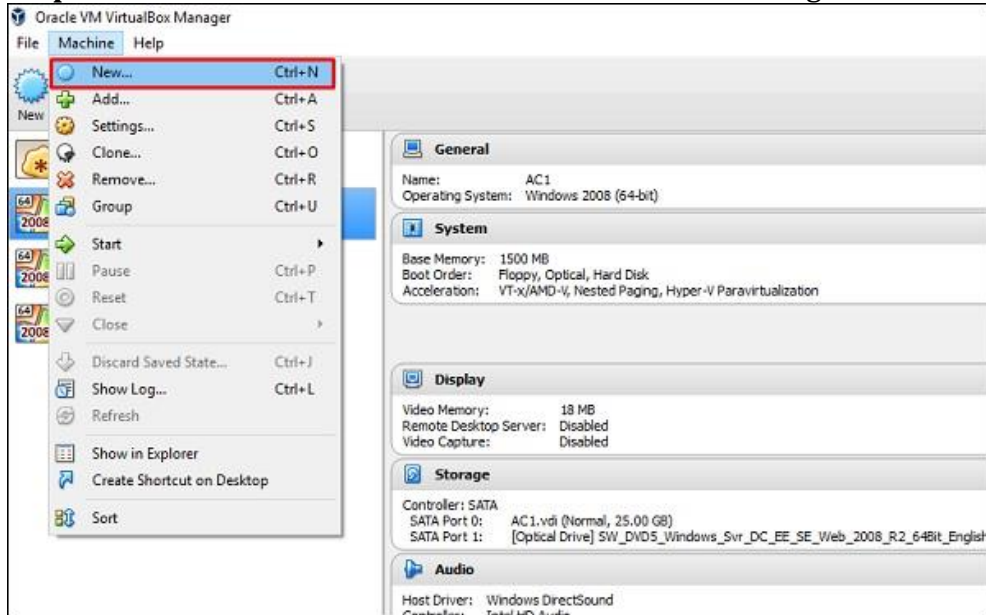
Now that we have successfully installed the Virtual Box, let's move on to the next step and install Kali Linux.

Step 1 – Download the Kali Linux package from its official website: <https://www.kali.org/downloads/>

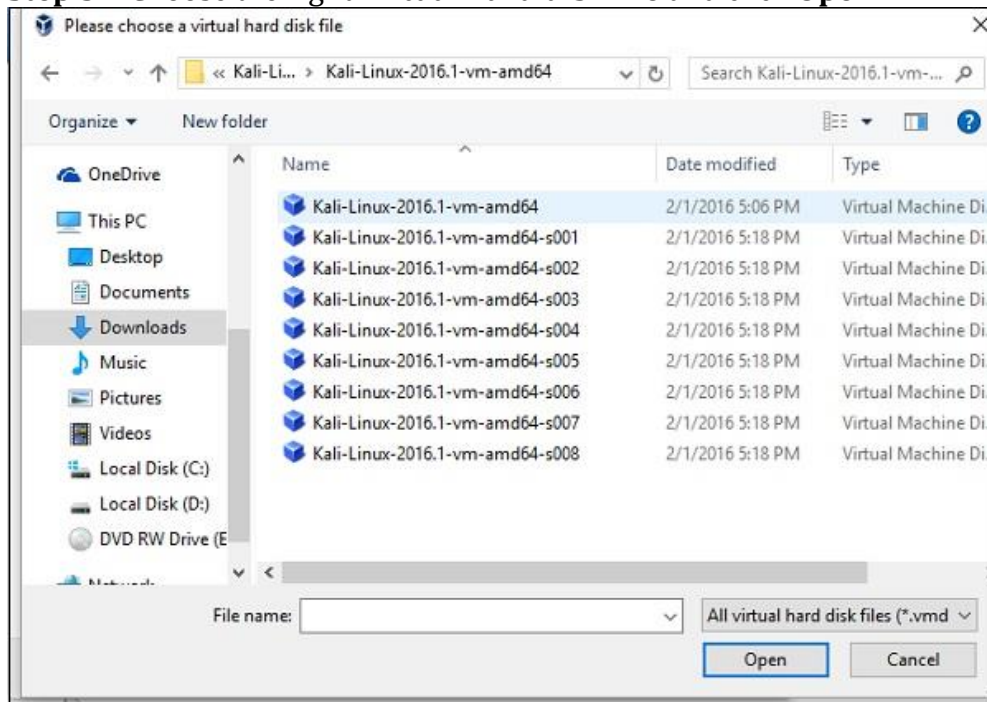


Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.0G	2016.1	2b49bf1e77c11ecb5618249ca69a46f23a6f5d2d
Kali Linux 32 bit VM PAE	Torrent	2.0G	2016.1	e71867a8bbf7ad55fa437eb7c93fd69e450f6759

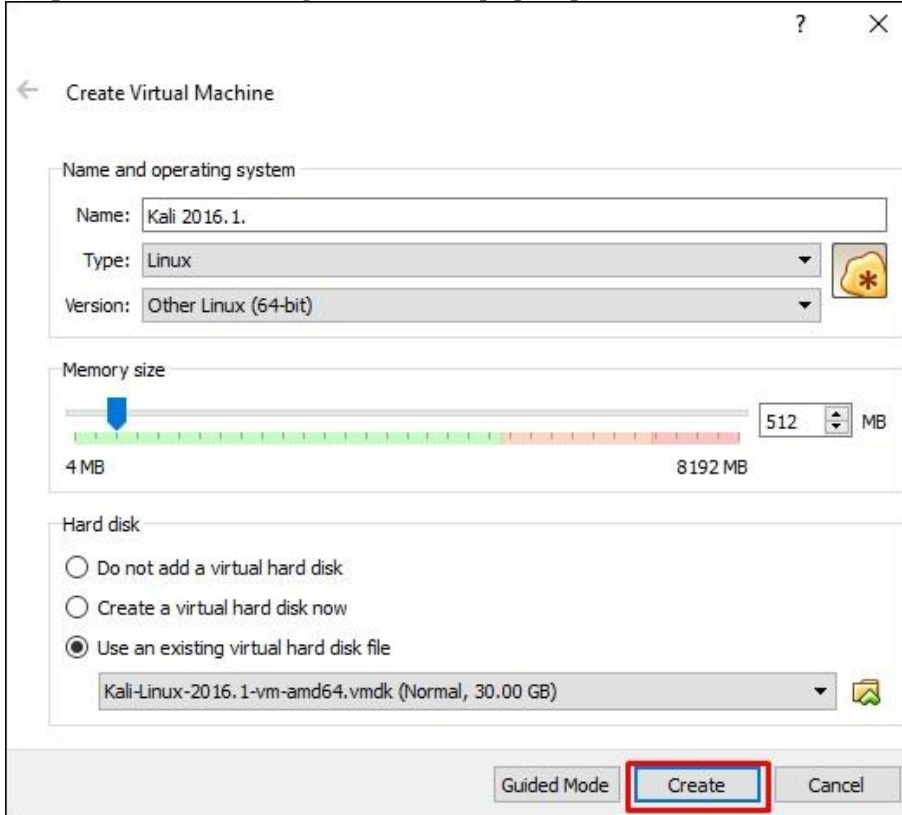
Step 2 – Click VirtualBox → New as shown in the following screenshot.



Step 3 – Choose the right virtual hard disk file and click Open.



Step 4 – The following screenshot pops up. Click the **Create** button.



Create Virtual Machine

Name and operating system

Name: Kali 2016.1.

Type: Linux

Version: Other Linux (64-bit)

Memory size

4 MB 8192 MB

512 MB

Hard disk

☐ Do not add a virtual hard disk

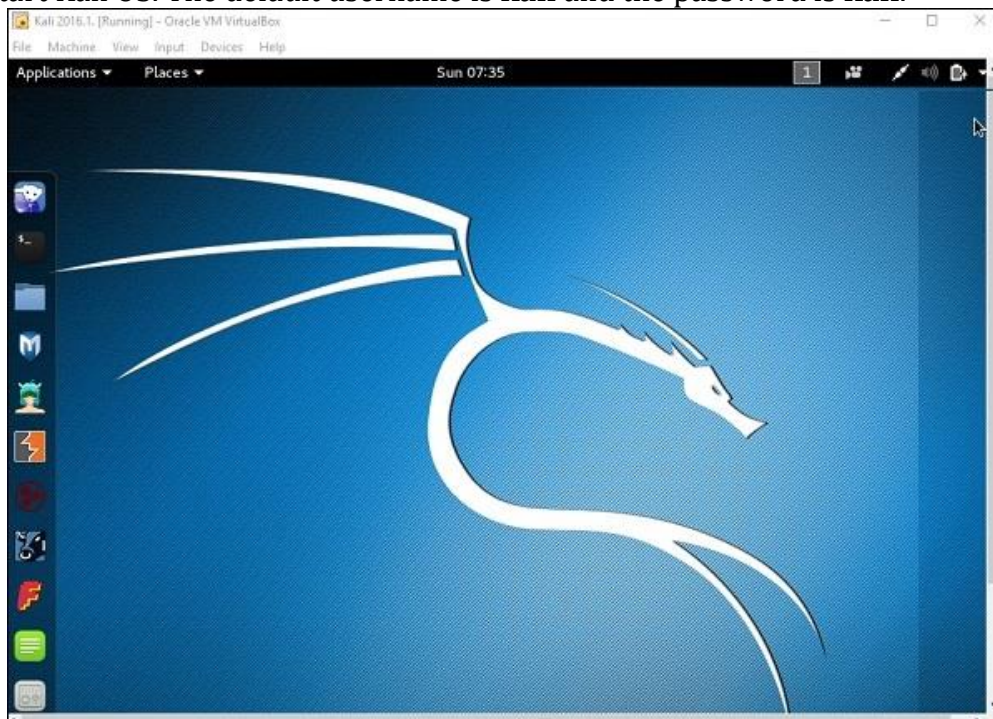
☐ Create a virtual hard disk now

☒ Use an existing virtual hard disk file

Kali-Linux-2016.1-vm-amd64.vmdk (Normal, 30.00 GB)

Guided Mode Create Cancel

Step 5 – Start Kali OS. The default username is **kali** and the password is **kali**.



Metasploit setup

- Log into **Kali Linux** machine and open a **Terminal** window.
- Start PostgreSQL database service to link with Metasploit:
`service postgresql start`
- Now type `msfconsole` to launch Metasploit.
`msfconsole`
- Check if Metasploit is connected to the database successfully:
`db_status`
[*] postgresql selected, no connection
- If you got this message, it means that database did not connected to msf properly. To fix this issue, type `exit` to quit Metasploit. Then, to initiate the database, type:
`msfdb init`
- Then, restart the postgresql service:
`service postgresql restart`
- Start Metasploit again and run the `db_status` to check the database status:
`msfconsole db_status`
[*] Connected to msf. Connection type: postgresql.
- Now the database is connected successfully to the msf.

hash-identifier

It is a tool that is used to identify types of hashes, meaning what they are being used for.

NMAP and ZenMAP

NMAP and ZenMAP are useful tools for the scanning phase of Ethical Hacking in Kali Linux. NMAP and ZenMAP are practically the same tool, however NMAP uses command line while ZenMAP has a GUI.

NMAP is a free utility tool for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

NMAP uses raw IP packets in novel ways to determine which hosts are available on the network, what services (application name and version) those hosts are offering, which operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, etc.

For more information, use this link: <https://nmap.org/book/man-os-detection.html>

Questions:

Ananth is running a reconnaissance on one of the systems – 10.0.2.28 on the network. As an investigator, your job is to see the details that the hacker will try to access and perform forensic investigation.

Task 1 (15 points)

Instructions:

1. Detect the OS type/version of the target host using nmap.
2. To scan all the TCP ports based on NMAP
3. Run the SYN scan in NMAP.

Task 2 (30 points)

Instructions

1. Find alive hosts
 - a. Scan the subnet using Nmap and save **output in XML** file called **GradedProject**.
 - b. Import the Nmap results from the database.
 - c. Show the hosts and their details discovered by Nmap type.
 - d. Scan to check the services running on this system – 10.0.2.28.
 - e. Display the whole list of the services running on the host.
2. Scan for open ports and services
 - a. Search for **portscan** modules.
 - b. Select the **scanner/portscan/syn**.
 - c. Show the module options.
 - d. Launch the module.
 - e. Find out the SMB version

Task 3 (5 points)

Instructions

In this task, you will practice the different password Cracking Tools in Kali Linux.

1. Hash-Identifier
 - a. Identify the following hashes using hash-identifier –
 - 098f6bcd4621d373cade4e832627b4f6
 - 8743b52063cd84097a65d1633f5c74f5
 - b89eaac7e61417341b710b727768294d0e6a277b

Submission Details:

Once complete the above tasks, take a screenshot of each task and submit the same. [Please make sure that command for each task is clearly visible on the screenshot]

Note: Please use the Sample Report Format docx file (on Olympus) to submit the project report.