**Lab 1: Kali Linux (Tiger Box)**

In this practical you will set up your lab PC for course related practical

**Objectives**

activities. The setup primarily involves the installation of relevant software tools.

**CLO**: 3

**Duration**: 60min+

* Lab PC

**Requirements**

* Lab Files: Software tools:

o Kali Linux

**Tasks**

* Task 1: Install Kali Linux
* Task 2: Customize Kali
* Task 3: Kali GUI
* Task 4: Kali Linux Terminal and Shell

**Lab Environment**

**Student Notes**

We will be working in a controlled lab environment where most of the activities will be carried out using Virtual Machines (VMs).

**Name: ID:**

## The Security Lab

|  |  |
| --- | --- |
|  | **The Security Lab Environment:**  It is important to understand that the security lab is a controlled security testing environment. You are NOT allowed to perform any type of intrusion or hacking activities outside the lab environment. The lab PC will be used as the main security workstation.  **Lab Resources:**   * **VM Workstation (or Player)**: This will be our main virtual machine software * **PC**: High-end PCs will be used. All software should be installed on these machines (RAM –Minimum 8GB –Recommended 16GB. Storage – Minimum 50GB –Recommended 100+GB) * **SW Tools**: Relevant software tools will be provided   **Student Requirements:**   * **Backup Disk**: It is highly recommended that you backup your lab work |



**Task 1: Install Kali Linux**



|  |  |
| --- | --- |
|  | **Task Objectives**  You will install Kali Linux as the Tiger Box for the course |

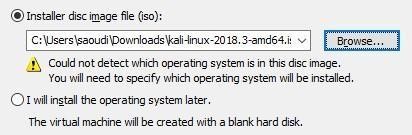
### About Kali Linux

|  |  |
| --- | --- |
|  | “Kali Linux is the new generation of the industry-leading BackTrack Linux penetration testing and security auditing Linux distribution. Kali Linux is a complete re-build of BackTrack from the ground up, adhering completely to Debian development standards.” Source and to learn more: <http://docs.kali.org/>  Kali Linux is a free open source toolbox with more than 600 penetration testing tools included. Kali Linux will be our main tiger box (toolbox) for the course.  Kali Linux is an open source project that is maintained and funded by Offensive Security. In addition to Kali Linux, Offensive Security also maintains the Exploit Database and the free online course, Metasploit Unleashed. |
|  | Screenshots and steps in this lab are based on Kali Linux 2018.3 AMD 64 bits, and VMWare Workstation 14 Pro. |

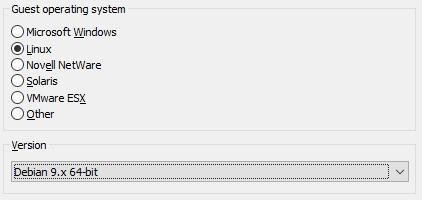
1. Download the latest Kali ISO image from the Kali website (**kali-linux- 2018.3amd64.iso** is the version used in this lab activity)
2. Open VMware Workstation and create a new virtual Machine (File  New Virtual

Machine…)

1. Keep **Typical** configuration and click **Next**
2. In the Guest Operating System page, select **Installer disk image file (iso)** and browse to select the newly downloaded **ISO** file, and click Next

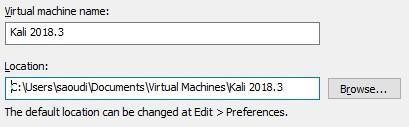
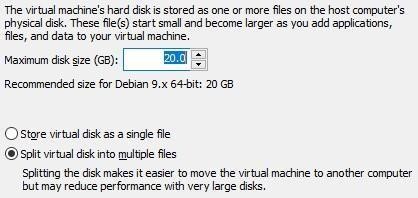


1. For the Operating System, select **Linux** and from the dropdown menu, select **Debian**

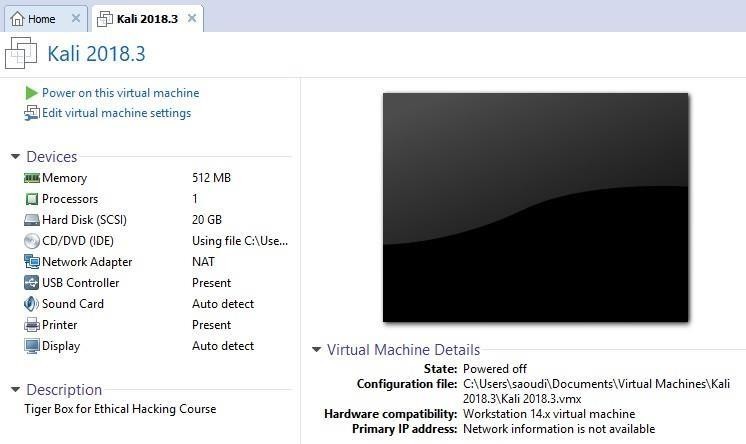
(any version since Kali is a ‘Debian-like’ distribution), and click **Next**

1. Type **Kali 2018.3** as the VM name and note the default location folder (don’t change it), then click **Next**

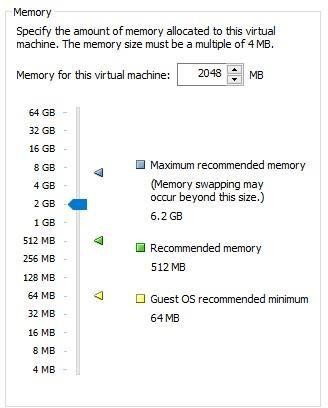
|  |  |
| --- | --- |
|  | The default folder is where all your VMs should be in case you copied or moved a machine later in the course. |

1. The default size of **20GB** should be enough. Keep the defaults and click **Next**
2. Verify the summary info and click **Finish**

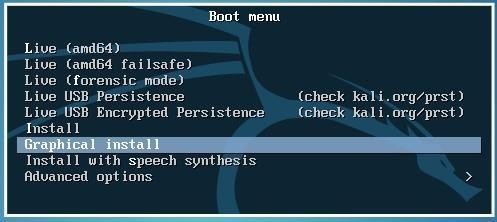
|  |  |
| --- | --- |
|  | We will change the memory (RAM) in the next step. The default of 512 MB is not enough. |



1. Click the **Edit virtual machine settings** to change the memory to 2048 MB (2GB) as shown below



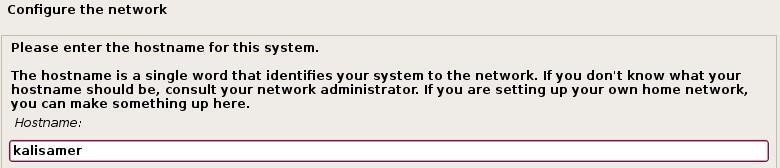
1. Click OK to save the changes
2. The VM is created but Kali is not yet installed on the virtual disk. In VMware Workstation, click the **Power on this virtual machine**
3. If you get a warning prompt, click Ok and in the boot menu, select the **Graphical install** option and hit enter

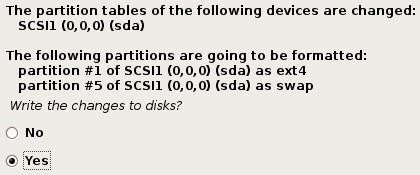


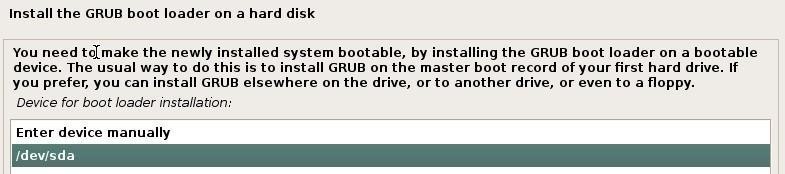
1. Leave the default **language** (English), **country** (OtherAsiaUnited Arab Emirates),

**locale** United States, and **keyboard** (American English)

1. For the **hostname**, type kaliyourname (e.g. kalisamer) and continue



1. Leave the domain name empty and **continue**
2. Type **password** (all lowercase) as the root password, re-enter and **continue**
3. Accept the default **clock** configuration
4. Accept the default **disk partition** configurations ( you need to click **continue** few times)
5. Select Yes to **write changes to disks** and **continue**
6. Let the system finish installing, and when done, select **No** for **network mirror**
7. Select **Yes** to install **GRUB boot loader** and continue to choose the device as shown below (**/dev/sda**)

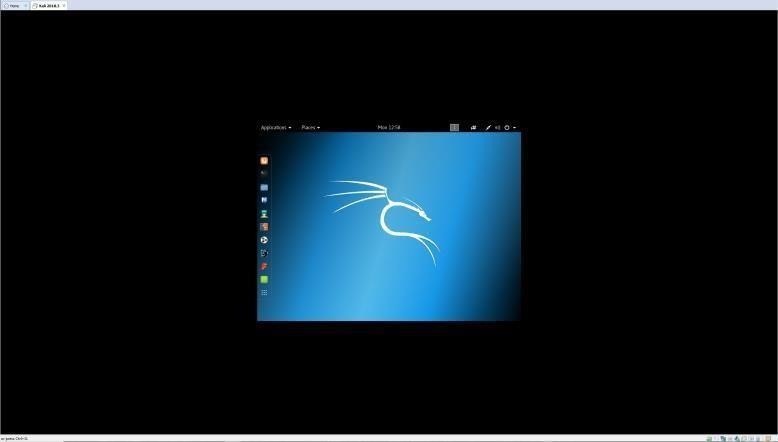


1. When the installation is complete, click **Continue** for the final cleanup
2. Click the **I Finished Installing** button at the bottom of your VMWare window. If you cannot see this button, ignore this step



1. The system will restart. Login using **root/password** as the credentials

|  |  |
| --- | --- |
|  | Notice that the Kali VM window will be relatively small and visually may not be very practical (depending on the resolution of your host computer).  Although there is an option to ‘AutoFit’ the guest window (View  Autosize), this will not work. There is a step we need to do before we can auto-fit. |

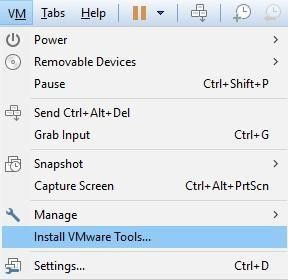


Kali VM Window

# [--End of Task 1--]

## Task 2: Customize Kali

|  |  |
| --- | --- |
|  | **Task Objectives**   * You will get familiar with the Kali GUI * You will customize Kali |

1. From VMWare, click the VM menu and select **Install VMware Tools**

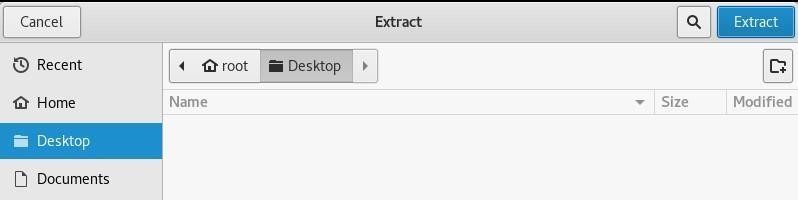
This will mount a virtual CD with the required tools



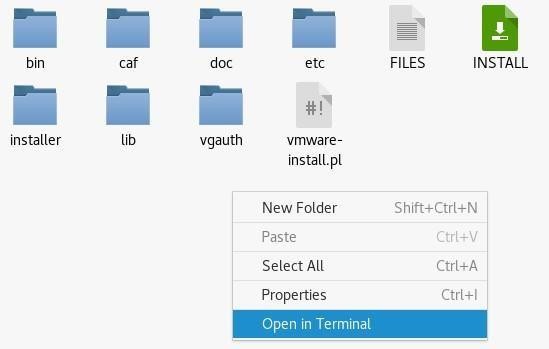
You will also get some help on what to do next

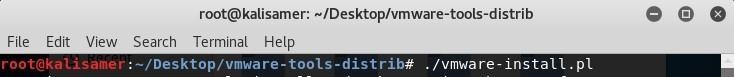
1. Double-click the VMware Tools CD icon on the desktop

This will open the contents of the tools CD

1. Locate the archive file (**tar.gz**)
2. Right click and **Open With Archive Manager**
3. In **Archive Manager**, click Extract and choose a location (e.g. Desktop)
4. Click the Extract button (top right corner)
5. Open the extracted folder

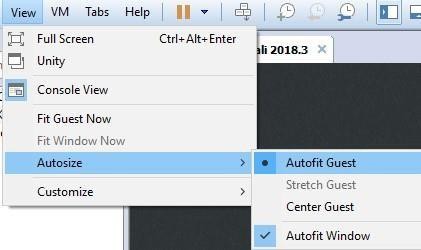
Extracted folder on the Desktop

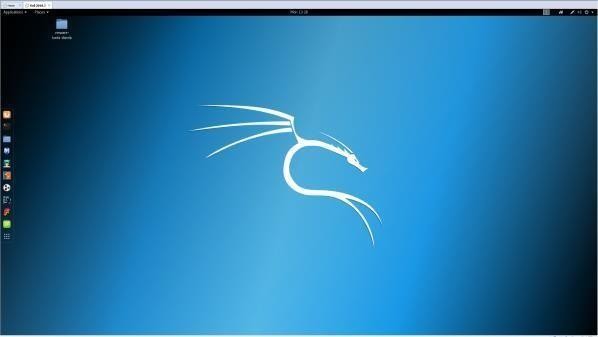


1. Right-click any empty point in the folder and click **Open in Ter**minal
2. In the terminal window, run the command shown below

**./vmware-install.pl**

1. During the installation, you will be prompted for file locations, accept the defaults by hitting Enter on each prompt
2. You will be asked for configuration questions, accept the default by hitting Enter on each prompt
3. When done, shutdown your Kali VM
4. If you haven’t done so already, select the **Autofit Guest** option as shown below



1. Start your Kali VM

Kali VM Window

1. Try to copy/paste or drag-and-drop files between your host computer and your guest VM

# [--End of Task 2--]

## Task 3: Kali GUI

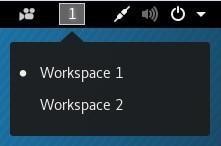


|  |  |
| --- | --- |
|  | **Task Objectives**  You will get familiar with the Kali GUI |

1. Open the web browser and ensure you have an internet connection
2. Get familiar with Kali’s user interface and answer the questions below

|  |  |
| --- | --- |
| **What is the name of**  **the web browser?** |  |
| **What is your**  **hostname?** |  |
| **What is your IP**  **address?** |  |
| **What command did you use to get the IP**  **address?** |  |
| **How many application**  **categories are in the Kali tiger box?** |  |
| **Under which category**  **can nmap be found?** |  |
| **Under which category can Wireshark be**  **found?** |  |
| **Under which category**  **can john be found?** |  |

1. Kali Linux supports what is known as workspace (shown below). Research Linux Workspace and write your findings in the space below:



|  |  |
| --- | --- |
| **What is a Linux Workspace?** |  |

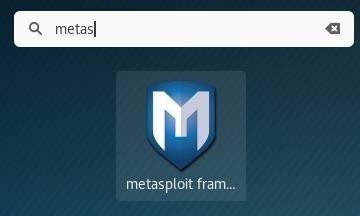
1. Find the icon shown below and answer the question

|  |  |
| --- | --- |
| **What is this icon used for?** |  |

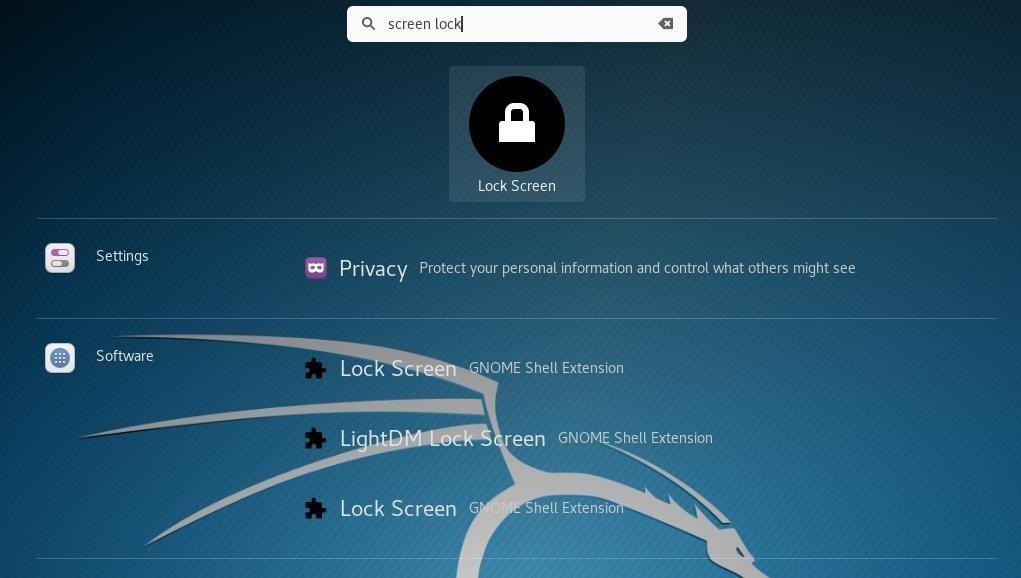
1. Click the Show Applications icon
2. Click All to show all applications

|  |  |
| --- | --- |
|  | Notice that the screenshot shows 3 pages of applications, and that they are searchable. |

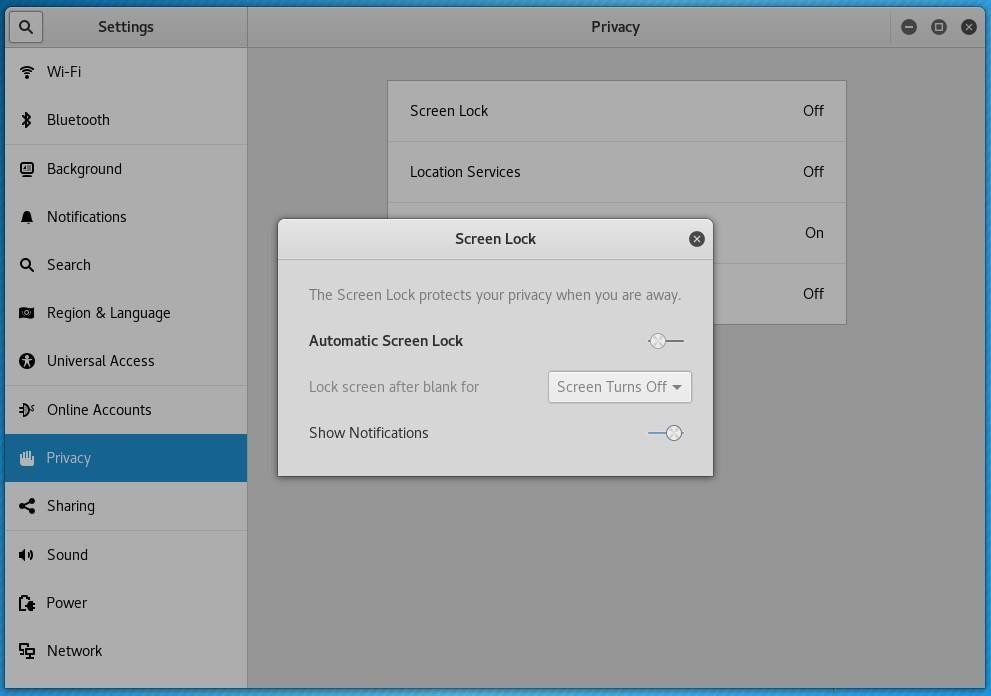
1. In the search field, type **metasploit** and notice how as you type, the application appears



1. Let’s turn off the screen lock in our Kali. Type **screen lock** in the search field and then select the **Privacy** setting



Select Privacy

1. Turn off the screen lock as shown below and then close the privacy settings window
2. **Independent Step**:

Change the power options so that the screen doesn’t turn off after 5 min (which is the default). Change it to Never

# [--End of Task 2--]

## Task 4: Kali Linux Terminal and Shell



|  |  |
| --- | --- |
|  | **Task Objectives**  You will use Linux commands and discover what they do |

|  |  |
| --- | --- |
|  | In Linux, the **Terminal** is a window that allows you to write commands and execute.  When the **Terminal** opens, it would have a program running in it called **bash**, which is a **shell** that can interpret and execute commands. The output is sent back to the Terminal.  A **Shell** is a command-line interpreter.  The location of **bash** is in the **bin** folder (**/bin/bash**). |

|  |  |
| --- | --- |
|  | Most of our work will be through the Terminal and its Shell, using commands. |

* 1. **Independent Step**:

Open a **Terminal** window and find out how you zoom in and out using keyboard shortcuts (Hint: Preferences)

|  |  |
| --- | --- |
|  | The two most important commands/utilities are: **man** and **help**  **man**: Linux man pages help to explain what each command can do. Each man page should give you a general overview of the command, its flags (options) and possibly an example of how to use it.  **help**: Linux help provides information about a function or command. |

|  |  |
| --- | --- |
|  | In practical exams, you are allowed to use the **man** pages and the **help** system. |

* 1. In your Terminal, open a new tab (not a new window), and run the following command: **man ifconfig** 3. Try: **help ifconfig** (did it work?)

1. **Independent Step**:

**Using man and/or help, find out about the following commands, and write down what each command does:**

|  |  |
| --- | --- |
| **clear** | Clears your screen |
| **cd** | Cd = change directory. If you use it alone it will take you  to the home directory. Also it can take you to specific directory. |
| **Ls** | It is for listing files in your current directory. |
| **Mkdir** | Create the DIRECTORY |
| **Tar** | an archiving program designed to store multiple files in a single file (an archive) |
| **Pwd** | Print the full filename of the current working directory. |

1. Type the following command
2. Type the following command



|  |  |
| --- | --- |
| **Is Linux case sensitive?** | yes |

1. Type the following command (note you should be inside the Desktop directory; also note the space)



1. Type the following command
2. Go back to the Desktop directory. What command did you type?

Cd Directory

1. What are the contents of the Desktop directory? And what command did you use?

ls, and I have only one file call (vmware-tools-distrib)

1. Type the following command (replace Samer with your name)
2. Type the following command (note that you should be in your name folder)



You must be on desktop to enter the cod tar -cf archive.tar Abdulla

1. Type the following command
2. Type the following command (note the space)



1. After the above command, try the **pwd** command again. What is the output?

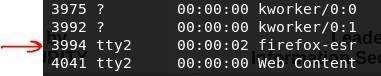
/

|  |  |
| --- | --- |
| **What is the difference between the following? cd .. cd /** | Cd .. one step back  Cd / return you to the home directory |

1. Using one command change the directory from the root **/** folder to the folder you created earlier on the Desktop (your name). What command did you use?

cd root/Desktop/Abdulla

1. Start the web browser
2. Minimize the browser but keep it open
3. Go back to the terminal window and clear it
4. Type the following command
5. Scroll down until you find firefox-esr and write down the PID (process ID):



1221 ?

1. Type the following command (basically, we filtering the output with results that contain “fire”)



It’s a faster way to get the PID

1. Now, we want to kill the **firefox** process using the **kill** command. Find out how it’s done. What command did you use?

kill 1221

# [--End of Task 4--]