**Lab Experiment 07**

**B. Tech CSF-CSE Semester III Course: Physical and IT Security**

**By: Dr. Gopal Singh Rawat**

**Objective is to**

* Learn Kali Linux Basics and Administration
* Add Victim Machine

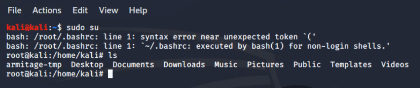
**Theory:**

* Kali Linux:
  + Open Source, Distribution OS for Penetration Testing & Forensics
  + Now Kali Linux has over 600 toolset & packages on Debian OS
* Powerful Platform for Vulnerability Assessment, Advanced Penetration Testing and also includes
  + Information Gathering
  + Vulnerability Analysis
  + Web Application Analysis
  + Database Assessment
  + Password Attacks
  + Wireless Attacks
  + Reverse Engineering
  + Exploitation Tools
  + Sniffing & Spoofing
  + Post Exploitation
  + Forensics
  + Reporting Tools
  + Social Engineering Tools
  + System Services

**Practice Activities:**

1. Start with simply opening the terminal 🡪 use Kali Linux 🡪 Go to the menu in the top-left corner, and search for ‘Terminal’, then click the icon to open it.
2. **Color Coding Terminal:**

If you do $ sudo su OR $ ls 🡪 you see just black and white



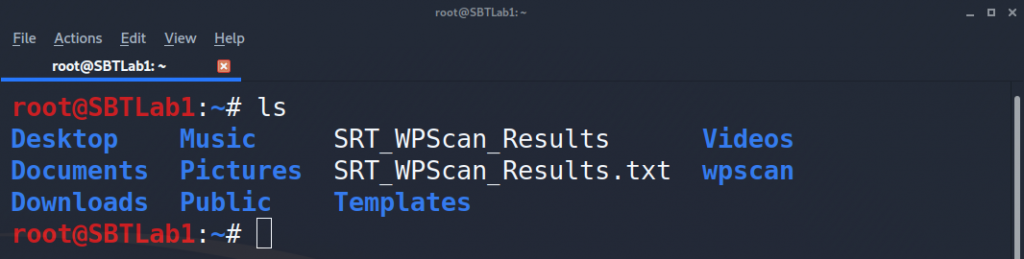
**To get colors on your terminal**

* **Edit Bash RC file** 🡪 **# leadpad ~/.bashrc**
* **Copy all from** [**https://github.com/redpython961/kali/blob/master/bashrc.txt**](https://github.com/redpython961/kali/blob/master/bashrc.txt)
* **Delete contents from existing BashRC file and paste from the Github file**
* **Close the Terminal & Reopen it. You should see colored details.**

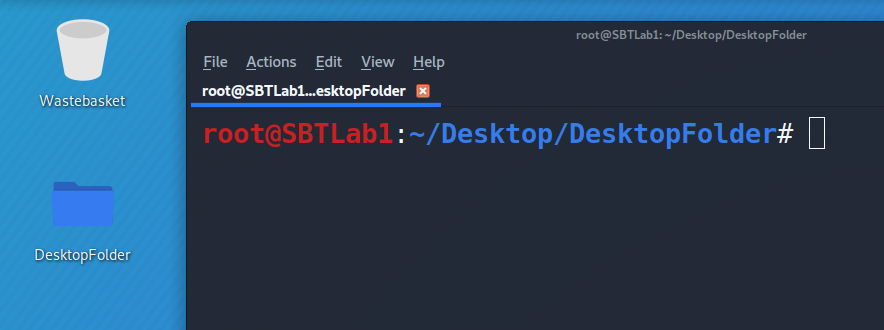


|  |  |
| --- | --- |
| **Color** | **Description** |
| Blue | Directories |
| Sky Blue | Symbolic Link |
| Red | Archived / Zip |
| Green/White | Executable |
|  |  |

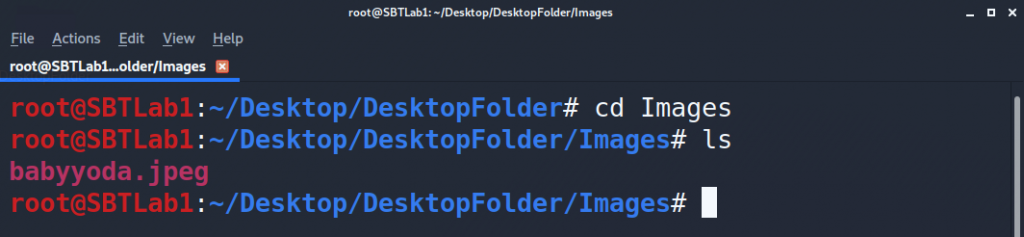
1. We started a terminal session that will be in the logged-in user’s directory (my account is ‘root’, so we are in the /root/ directory. We can see which files are in this directory by using the command ls which is used for listing contents of the current folder. In the screenshot below we can see other directories in blue, and text files in white.



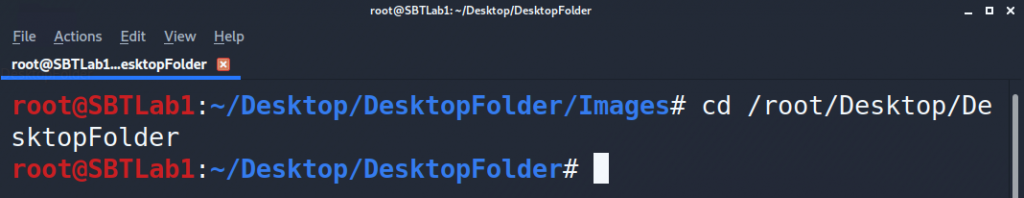
1. Let’s take a look at our testing directory named ‘DesktopFolder’. In the below screenshot on the left you can also see the folder icon on the Desktop, and on the right you can see that our terminal is currently positioned in the Desktop directory, then inside the DesktopFolder directory (/Desktop/DesktopFolder/).

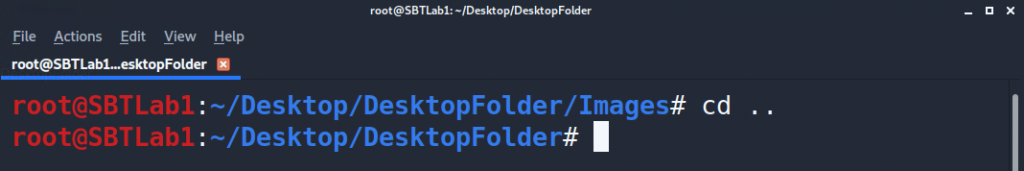


1. To move around, we need to use the "cd" command, which is short for change directory. We know the sub-folder is named **Images**, so let’s use "cd Images" and then list the contents with "ls". Once we move into ***/Desktop/DesktopFolder/Images*** we can see there’s a .jpeg image file named ‘babyyoda.jpeg’.

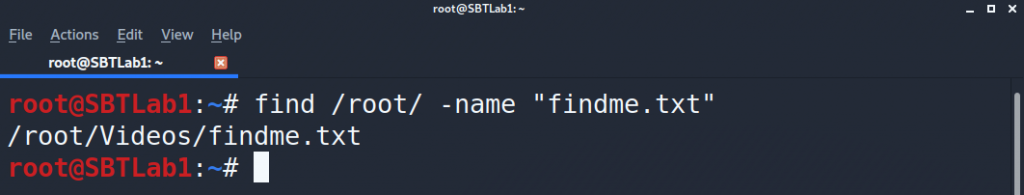


1. To go back to ***/Desktop/DesktopFolder/*** we can either use the command "cd /root/Desktop/DesktopFolder" to move directly to the specified location, or we can simply go back to the previous directory using "cd ..". In the below screenshots the left image shows the first command, and the right image shows the second command.





1. Now we try to find a text file called ‘FindMe.txt’ that is under the account ‘root’, so we’ll use the command find /root/ -name "findme.txt".



1. **Basic Hygiene for Kali Linux:**

* **After downloading and initial default installation – run as Virtual Machine or Dual Boot system**

|  |  |
| --- | --- |
| **Display User Name of current user** | **root@kalilinux:~# whoami** |
| **Display current data and time** | **root@kalilinux:~# date** |
| **Displays current Working Directory** | **root@kalilinux:~# pwd** |
| **Change directory** | **root@kalilinux:~# cd Desktop** |
| **Go Back to the same directory** | **root@kalilinux:~# cd** |
| **List all contents including hidden directory** | **root@kalilinux:~# ls –al /desktop** |
| **Create new directory** | **root@kalilinux:~# mkdir Desktop/New** |
| **Add new file inside the newly created directory** | **root@kalilinux:~# touch Desktop/New/NewFile.txt** |
| **Clear Screen** | **root@kalilinux:~# clear** |
| **Display uptime of system** | **root@kalilinux:~# uptime** |
| **Display Linux OS & Version** | **root@kalilinux:~# uname –r** |
| **Display Total, Available, Shared, Buffer & Used RAM** | **root@kalilinux:~# free –t** |
| **Display all users** | **root@kalilinux:~# cd /etc/passwd** |
| **Shutdown the system immediately** | **root@kalilinux:~# init 0** |
| **Reboot the system immediately** | **root@kalilinux:~# reboot** |
| **Display network interface status** | **root@kalilinux:~# ifconfig** |
|  |  |
| **Update Kali Linux Source List**  **Update Sources.list file with repositories from** | **root@kalilinux:~# cd ..**  **root@kalilinux:/# cd etc/apt**  **root@kalilinux:/etc/apt# gedit sources.list**  [**https://docs.kali.org/generl-use/kali-linux-sources-list-repositories**](https://docs.kali.org/generl-use/kali-linux-sources-list-repositories) **OR Add the following lines:**  deb http://http.kali.org/kali kali-rolling main contrib non-free  deb-src http://http.kali.org/kali kali-rolling main contrib non-free  deb http://http.kali.org/kali sana main non-free contrib  deb http://security.kali.org/kali-security sana/updates main contrib non-free  deb-src http://http.kali.org/kali sana main non-free contrib  deb-src http://security.kali.org/kali-security sana/updates main contrib non-free  deb http://old.kali.org/kali moto main non-free contrib  deb-src http://old.kali.org/kali moto main non-free contrib |
| **Update Kali Linux OS** | **root@kalilinux:~# sudo apt-get update** |
| **Install GIT 🡪 download (clone) from GIT Repository for open source version controls** | **root@kalilinux:~# apt-get install git** |
| **Update Kali Linux** | **root@kalilinux:~# apt-get update** |
| **Add user (I call the new user as NOTROOT**  Enter password twice, name, room number, work & home phone details | **root@kalilinux:~# useradd notroot** |
| **Add NOT ROOT user to Admin group (SU Permissions)** | **root@kalilinux:~# usermod –aG sudo notroot** |
| **Install Terminal Multiplexer**  Run multiple scripts / commands in one window at the same time | **root@kalilinux:~# apt install tilix**  **root@kalilinux:~# tilix** |
| **Download and install packages with best / updated features**  **Kali Meta Packs 🡪**  **Install RFID 🡪**  **Install Multiple Tools 🡪**  **Upgrade Kali 🡪** | **https://www.kali.org/news/kali-linux-metapackages/**  **root@kalilinux:~# sudo apt update && apt install kali-linux-rfid**  **root@kalilinux:~# apt-get install maltego metasploit-framework burpsuite wireshark aricrack-ng**  **root@kalilinux:~# apt-get update && apt-cache search kali-linux**  **OR**  **root@kalilinux:~# sudo apt update**  **root@kalilinux:~# apt list upgradable**  **root@kalilinux:~# sudo apt upgrade** |

1. **Kali Linux Services:**

* **SSH: allows remote access** 
  + **To start/stop: # service ssh start**
  + **To check: # netstart antp|grep ssh**
  + **To start automatically at boot/reboot: # update.rc.d ssh enable // disable**
* **HTTP: Host web site**
  + **To start/stop: # service apache2 start**
  + **To check: # netstat –antp|grep apache2**
  + **To start automatically at boot/reboot: # update.rc.d http enable // disable**
* **Install services not available in Linux Distribution**
  + **To install: # apt-get install vsftpd**
  + **To start/stop: # service vsftpd start**
* [**https://www.udemy.com/course/kalipentest/learn/lecture/12295462#overview**](https://www.udemy.com/course/kalipentest/learn/lecture/12295462#overview)

1. **Setup Victim Windows 10 Machine**

* Go to[**https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/**](https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/)
* Download the Windows 10 OS as per your Virtualization App (VMWare, Virtual Box …)
* Note:
  + **These virtual machines expire after 90 days**.
  + Recommend setting a snapshot when you first install the virtual machine, that you can roll back to later.
  + Mac users will need to use a tool that supports zip64, like [The Unarchiver](http://unarchiver.c3.cx/unarchiver), to unzip the files.
  + The password to your VM is "Passw0rd!"
* Save the Windows 10 IOS on your VMware storage folder, import the file
* Edit the hardware settings (RAM, CPU..) as required

**Lab #07 Activities: Perform the above steps for your Kali Linux Machine.**